Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BENGALURU SINGAPORE NEW DELHI NEW YORK GIFT CITY BOSTON

Research

Cross-Border Compliance in Fintech

Navigating India's DPDPA and the U.S. Sectoral Regime towards a framework for the BFSI Sector

April 2026

Research

Cross-Border Compliance in Fintech

Navigating India's DPDPA and the U.S. Sectoral Regime towards a framework for the BFSI Sector

April 2026

DMS Code: 151844.2

FT INNOVATIVE LAWYERS 2019
FINANCIAL TIMES
ASIA-PACIFIC WINNER

Ranked as the 'Most Innovative Indian Law Firm' in the prestigious FT Innovative Lawyers Asia Pacific Awards for multiple years. Also ranked amongst the 'Most Innovative Asia Pacific Law Firm' in these elite Financial Times Innovation rankings.

Chambers AND PARTNERS

IFLR1000

The LEGAL 500

BENCHMARK LITIGATION

asialaw

WWL

ASIAN LEGAL BUSINESS

INDIA BUSINESS LAW JOURNAL

INDIA BUSINESS LAW JOURNAL THE A LIST 2023 2024 LAW ASIA

INDIA BUSINESS LAW JOURNAL DEALMAKER 2023 LAW ASIA

Mergermarket An Acuris company

ITR WORLD TAX

iel ELITE

BUSINESS TODAY

THE NATIONAL LAW REVIEW

equalFi

ILA IDEX LEGAL AWARDS

LEGAL ERA BY THE PEOPLE. FOR THE PEOPLE. OF THE PEOPLE

LawWiser .com

Disclaimer

Contact

For any help or assistance please email us on **concierge@nishithdesai.com**
or visit us at **www.nishithdesai.com**.

Acknowledgements

Avi Konduri
avikonduris@gmail.com

Vaibhav Parikh
vaibhav.parikh@nishithdesai.com

Contents

List of Abbreviations

Abbreviation	Full Form
AG	Attorney General
AGs	Attorneys General
AI	Artificial Intelligence
AML	Anti-Money Laundering
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
BCBS 239	Basel Committee on Banking Supervision Principles for Effective Risk Data Aggregation and Risk Reporting
BCG	Boston Consulting Group
BCRs	Binding Corporate Rules
BFSI	Banking, Financial Services, and Insurance
BIS	Bank for International Settlements
BSA	Bank Secrecy Act / BSA | The Software Alliance
CBPR	Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act
CDPA	Consumer Data Protection Act
CERT-In	Indian Computer Emergency Response Team
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CISO	Chief Information Security Officer
CNP	Card-Not-Present
CoF	Card-on-File
CoFT	Card-on-File Tokenisation
CPA	Colorado Privacy Act
CPPA	California Privacy Protection Agency
CPRA	California Privacy Rights Act
CTDPA	Connecticut Data Privacy Act
DPBI	Data Protection Board of India
DPDP	Digital Personal Data Protection
DPDPA	Digital Personal Data Protection Act, 2023
DPIA	Data Protection Impact Assessment
DPIAs	Data Protection Impact Assessments
DSCI	Data Security Council of India
EDPB	European Data Protection Board
EDR	Endpoint Detection and Response
EU	European Union
EY	Ernst & Young
FATF	Financial Action Task Force
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
Fed	Federal Reserve
FFIEC	Federal Financial Institutions Examination Council
FICCI	Federation of Indian Chambers of Commerce and Industry
FinCEN	Financial Crimes Enforcement Network
FTC	Federal Trade Commission
G20	Group of Twenty
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act

Abbreviation	Full Form
IAMAI	Internet and Mobile Association of India
ICT	Information and Communications Technology
IMF	International Monetary Fund
INR	Indian Rupees
IRDAI	Insurance Regulatory and Development Authority of India
ISO	International Organization for Standardization
ISO 20022	International Organization for Standardization 20022 Financial Messaging Standard
IT	Information Technology
IT Act	Information Technology Act, 2000
KYC	Know Your Customer
MDL-668	Insurance Data Security Model Law (Model Law No. 668)
MFA	Multi-Factor Authentication
MGA	Managing General Agent
MoR	Merchant of Record
NAIC	National Association of Insurance Commissioners
NASSCOM	National Association of Software and Service Companies
NBFC	Non-Banking Financial Company
NIC	National Informatics Centre
NPI	Nonpublic Personal Information
NPL	National Physical Laboratory
NTP	Network Time Protocol
NYCRR	New York Codes, Rules and Regulations
NYDFS	New York Department of Financial Services
OCC	Office of the Comptroller of the Currency
OECD	Organisation for Economic Co-operation and Development
ORF	Observer Research Foundation
PA	Payment Aggregator
PAs	Payment Aggregators
PMLA	Prevention of Money Laundering Act, 2002
RBI	Reserve Bank of India
RFPA	Right to Financial Privacy Act
SaaS	Software-as-a-Service
SDF	Significant Data Fiduciary
SDFs	Significant Data Fiduciaries
SEC	Securities and Exchange Commission
SOC	Security Operations Center
SOCs	Security Operations Centers
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TDS	Tax Deducted at Source
TR	Token Requestor
TRs	Token Requestors
UCPA	Utah Consumer Privacy Act
UPI	Unified Payments Interface
U.S.	United States
USD	United States Dollar
VCDPA	Virginia Consumer Data Protection Act
VDA	Virtual Digital Asset
VDAs	Virtual Digital Assets
VPN	Virtual Private Network

Executive Summary

This paper presents a comparative legal and regulatory analysis of data protection frameworks in the Banking, Financial Services, and Insurance (BFSI) sectors of India and the United States, with particular focus on the challenges facing cross-border fintech firms. As digital finance continues to globalize, the ability of firms to comply with divergent national privacy regimes has become a central concern for operational scalability, infrastructure design, and regulatory strategy. This analysis is especially useful as firms today increasingly seek to operate across jurisdictions with fundamentally different legal philosophies and enforcement cultures. The purpose of this paper is thus to map the structural, doctrinal, and institutional differences between the Indian and U.S. regulatory approaches, and to assess their implications for compliance, risk management, and market entry strategies for fintech firms operating across both jurisdictions.

Briefly, India's regulatory architecture is characterized by a co-regulatory and vertically layered system. The Digital Personal Data Protection Act, 2023 (DPDPA)[1] establishes a horizontal, rights-based framework built on principles of consent, purpose limitation, and accountability. However, sectoral regulators, particularly the Reserve Bank of India (RBI)[2], the Insurance Regulatory and Development Authority of India (IRDAI)[3], and the Indian Computer Emergency Response Team (CERT-In)[4], retain robust independent authority. As a result, BFSI entities must simultaneously comply with RBI's data localization mandate for payments[5], IRDAI's local storage rules for insurance records[6], and CERT-In's cybersecurity breach reporting protocols[7], creating overlapping but non-derogable obligations. Since the original draft was written, the direction of travel in India has become clearer: the country has operationalised its data-protection architecture through final rules and the formal establishment of the Data Protection Board of India.[8]

In contrast, the United States adopts a sectoral and federated approach to financial data regulation. The Gramm-Leach-Bliley Act (GLBA)[9] forms the federal baseline for privacy and security in the BFSI sector through its Privacy, Safeguards, and Pretexting Rules. However, enforcement is dispersed across multiple agencies, including the Federal Trade Commission (FTC), federal banking regulators (OCC, Fed, FDIC), and state-level actors such as attorneys general and regulators like the New York Department of Financial Services (NYDFS)[10]. The U.S. framework is notably flexible regarding cross-border data transfers, relying on contractual safeguards rather than geographic restrictions, but imposes compliance complexity through state-level privacy laws such as the CPRA[11] and VCDPA[12] that may apply outside GLBA's scope.

1 Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extraordinary, Part II, sec. 1 (Aug. 11, 2023).

2 Reserve Bank of India, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-2018, Storage of Payment System Data (Apr. 6, 2018).

3 IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3, Gazette of India, No. IRDA/Reg/20/107/2015 (July 31, 2015).

4 Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022).

5 I Reserve Bank of India, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-2018, Storage of Payment System Data (Apr. 6, 2018).

6 IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3, Gazette of India, No. IRDA/Reg/20/107/2015 (July 31, 2015).

7 Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022).

8 Digital Personal Data Protection Rules, 2025; Ministry of Electronics and Information Technology Notification establishing the Data Protection Board of India, 13 Nov. 2025; National Conference of State Legislatures, Summary 2024 Consumer Data Privacy Legislation; Consumer Financial Protection Bureau, Personal Financial Data Rights (updated Jan. 2026).

9 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018).

10 New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500 (2023).

11 Cal. Civ. Code §§ 1798.100–1798.199 (2023).

12 Va. Code Ann. § 59.1–581.5(A)(1) (2023).

This paper thus argues that regulatory fragmentation and compliance asymmetry across the two jurisdictions present material challenges for cross-border fintech firms. These include increased infrastructure costs, heightened breach management obligations, and the need to construct segmented compliance architectures. All these particularly impact U.S.-based fintech firms expanding into India, who must contend with non-negotiable localization and reporting rules. To address these challenges, the paper recommends aligning compliance frameworks with global standards such as the OECD Privacy Guidelines[13], FATF[14], and BCBS 239[15], and advancing bilateral or multilateral interoperability mechanisms, particularly in the BFSI domain, where data is both commercially vital and legally sensitive.

13 Financial Action Task Force, Guidance on Digital Identity (2020).

14 Financial Action Task Force, Guidance on Digital Identity (2020).

15 Basel Committee on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239) (2013).

India: Statutory and Horizontal Framework (DPDPA, 2023)

The Digital Personal Data Protection Act, 2023 (**"DPDPA"**) marks India's formal entry into a comprehensive, rights-based data governance regime, with significant implications for the BFSI sector. Enacted pursuant to legislative powers under Article 246 of the Constitution, the DPDPA applies to the processing of digital personal data within the territory of India and extraterritorially to processing carried out outside India if it is in connection with the offering of goods or services to data principals in India.[1] The Act represents a shift from sectoral and executive-order-based data governance to a more structured statutory regime that recognizes individual privacy as a fundamental right, following the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India.[2]

The Act is built around several core data protection principles:

- **Notice**: Data fiduciaries must provide a clear and itemized notice to the data principal prior to or at the time of data collection. The notice must explain the nature of personal data to be collected, the purposes of processing, the data retention policy, grievance redressal mechanism, the categories of processors with whom data will be shared, and the intended cross-border transfers, if any.[3]
- **Consent:** The default basis for lawful processing is free, specific, informed, unconditional, and unambiguous consent. The request for consent must be presented in clear language and separated from other terms and conditions. Processing without consent is permitted only in narrowly defined "legitimate use" scenarios, such as compliance with law, performance of state functions, or for medical emergencies.[4]
- **Purpose Limitation and Data Minimization**: Personal data must be processed only for the specified purpose for which consent was obtained or the legitimate use was claimed. Collection must be limited to data necessary for that purpose, and processing must cease once the purpose is fulfilled.[5]
- **Storage Limitation and Accuracy**: Fiduciaries are required to ensure data is accurate and up to date, retained only for as long as necessary to satisfy the purpose, and then erased unless required to be retained under law or for legal claims.[6]
- Security Safeguards: Appropriate technical and organizational measures must be employed to prevent unauthorized access, disclosure, alteration, or destruction of personal data.[7]

Importantly, the DPDPA does not establish a whitelist-based adequacy system for cross-border data transfers, as in the European Union. Instead, Section 16 permits the transfer of personal data outside India by default, unless the Central Government issues a notification restricting such transfers to specified countries or territories.[8] It is important to note, however, that the notified Rules do not create a public adequacy whitelist. Instead, Rule 15 permits transfers outside India subject to any general or special order of the Central Government specifying requirements concerning the making available of personal data to a foreign State,

1 The Digital Personal Data Protection Act, No. 22 of 2023, § 3, Gazette of India, Extraordinary, Part II, sec. 1 (Aug. 11, 2023).
2 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3 DPDPA § 5.
4 DPDPA §§ 6–7.
5 DPDPA §§ 8–9.
6 DPDPA §§ 9–10.
7 DPDPA § 9.
8 DPDPA § 16.

or to a person or entity under that State's control. [9] This "negative list" model provides regulators with strategic discretion, including the power to restrict transfers based on national security, reciprocity, or absence of robust enforcement in the destination country. The draft-rule stage has now been overtaken. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025 in phased form: Rules 1, 2, and 17 to 21 took effect immediately; Rule 4 took effect after one year; and Rules 3, 5 to 16, and 22 to 23 take effect after eighteen months. Accordingly, as of March 2026, the DPDP framework is no longer merely prospective, but only partly operative. [10]

The Act defines key entities and roles:

- "Data Fiduciary" means any person who determines the purpose and means of processing personal data. [11]
- "Data Principal" refers to the individual to whom the data relates. [12]
- "Consent Manager" is a third-party entity registered with the Board, acting as a neutral interface for data principals to manage their consents. The final Rules now specify that a Consent Manager must be a company incorporated in India, and that its interoperable platform must be independently certified against data protection standards and assurance frameworks published by the Board.

The Data Protection Board of India, established under Chapter V, is the primary regulatory body with adjudicatory, enforcement, and supervisory functions. [13] The Board may initiate proceedings on complaints, issue directions for compliance, impose civil penalties up to ₹250 crore per breach, [14] and order blocking of repeat offender platforms in egregious cases. [15] The Board also oversees voluntary undertakings and alternative dispute resolution, recognizing the need for efficient enforcement in commercial contexts. [16] The Central Government has formally established the Data Protection Board of India, fixed its head office in the National Capital Region, and separately notified that the Board shall consist of four members. [17]

Importantly, Significant Data Fiduciaries (**"SDFs"**), identified under Section 10 based on factors such as volume and sensitivity of personal data processed, risk to rights of data principals, and potential impact on the sovereignty and integrity of India, are subject to additional obligations:

- Appointment of a Data Protection Officer based in India; [18]
- Performance of periodic Data Protection Impact Assessments and independent data audits; [19]
- Maintenance of more stringent records and internal grievance redressal mechanisms. [20]

The DPDPA coexists with sector-specific regulatory frameworks. Section 3 of the Act explicitly preserves more stringent obligations under other laws, which means that for BFSI firms, DPDPA compliance does not override

9 DPDPA §§ 9–10.

10 Digital Personal Data Protection Rules, 2025; Notification S.O. 5082(E), 13 Nov. 2025.

11 DPDPA § 2(i). DPDPA § 2(j). DPDPA § 2(e). DPDPA §§ 18–27. DPDPA § 33. DPDPA § 37. DPDPA § 32. DPDPA § 10(1)(a). DPDPA § 10(1)(b)–(c). Ibid. NASSCOM, Comments on Draft DPDPA Rules (2024), at 6. DPDPA § 15.

12 DPDPA § 2(j).

13 DPDPA §§ 18–27.

14 DPDPA § 33.

15 DPDPA § 37.

16 DPDPA § 32.

17 Ministry of Electronics and Information Technology Notification establishing the Data Protection Board of India, 13 Nov. 2025; Ministry of Electronics and Information Technology Notification on number of members, 13 Nov. 2025.

18 DPDPA § 10(1)(a).

19 DPDPA § 10(1)(b)–(c).

20 Ibid.

the RBI's 2018 payment data localization circular, the IRDAI (Maintenance of Insurance Records) Regulations, 2015, or the CERT-In Cybersecurity Directions, 2022.[21] This creates a dual compliance burden, whereby fintech firms must navigate both horizontal obligations under the DPDPA and vertical sectoral mandates.

While the Act does not create special rules for financial data, in practice, overlap with financial regulators' mandates results in enhanced scrutiny of BFSI players, especially those offering consumer-facing digital payment, lending, or insurance products. Furthermore, under Section 15, the Central Government may exempt certain classes of data fiduciaries, such as startups or offline-only processors, from specific obligations; however, such exemptions have not yet been finalized.[22]

Lastly, the final Rules partially resolve the paper's earlier uncertainty on breach timing. Rule 7 requires a Data Fiduciary, upon becoming aware of a personal data breach, to notify affected Data Principals in a concise, clear and plain manner without delay, and to notify the Board without delay, followed within seventy-two hours by updated and detailed information unless the Board allows more time. The Rules also require Data Fiduciaries and Consent Managers to maintain grievance-redressal systems capable of responding within a reasonable period not exceeding ninety days.[23]

21 NASSCOM, Comments on Draft DPDPA Rules (2024).

22 DPDPA § 15.

23 DPDPA.

Sectoral Compliance in India's BFSI Ecosystem: RBI, IRDAI, and CERT-In

India's regulatory regime for the Banking, Financial Services, and Insurance (BFSI) sector can be characterized as a co-regulatory structure that overlays horizontal privacy legislation with sector-specific mandates. This is because although the Digital Personal Data Protection Act, 2023 (**"DPDPA"**) applies horizontally across sectors, it explicitly preserves the authority of sectoral regulators such as the Reserve Bank of India (**"RBI"**) and the Insurance Regulatory and Development Authority of India (**"IRDAI"**), each of which has issued binding obligations, particularly in areas of data localization and cybersecurity.[1] These are further supported by directions issued by the Indian Computer Emergency Response Team (**"CERT-In"**) under the Information Technology Act, 2000, which apply to all digital service providers, including those in the BFSI domain.[2]

As a result, fintech firms operating in India must simultaneously comply with the DPDPA's general obligations, including purpose limitation, data minimization, notice, and consent requirements, and with more sector-specific directives that frequently impose more stringent duties.[3] For instance, the RBI mandates that payment data be stored exclusively in India and prohibits unauthorized storage of card credentials. Moreover, the IRDAI requires insurers to keep all policyholder records on servers physically located within Indian territory.[4] Finally, the CERT-In's 2022 guidelines also mandate near-immediate cybersecurity incident reporting and domestic log retention.[5]

The problem then is that these frameworks are enforced independently, often without formal harmonization, leading to cumulative compliance obligations. As noted by industry observers, co-regulatory friction remains a structural reality for FinTechs, given the multiple verticals of enforcement.[6] Accordingly, the sector's regulatory complexity extends beyond mere duplication and into areas of inter-agency coordination, operational design, and cross-border infrastructure strategy.

I. RBI Data Localization Mandate (2018 Onward)

India's most impactful sectoral data protection mandate originated with the RBI's 2018 circular titled Storage of Payment System Data. Issued under the Payment and Settlement Systems Act, 2007, the circular mandates that "all system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India".[7] This includes transaction details, customer credentials, payment instructions, and data logs. Although cross-border processing is permitted for settlement purposes, the data must be deleted from foreign systems and repatriated to Indian servers within 24 hours.[8]

1 Digital Personal Data Protection Act, No. 22 of 2023, § 3, Gazette of India, Extraordinary, Part II, sec. 1 (Aug. 11, 2023); Nishith Desai Assocs., India's Flourishing Fintech Flambeau 10 (2025).

2 Information Technology Act, No. 21 of 2000, § 70B.

3 DPDPA §§ 5–9.

4 RBI, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-2018 (Apr. 6, 2018); IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3.

5 CERT-In, Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), ¶¶ 4(a), 4(g).

6 NASSCOM, Comments on Draft Rules under the Digital Personal Data Protection Act, 2023 6 (Mar. 5, 2025).

7 RBI, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-2018, ¶ 2 (Apr. 6, 2018).

8 Ibid. ¶ 3.

This directive applies broadly to all payment system operators, including card networks (e.g., Visa, Mastercard), e-wallets, banks, and non-bank financial companies. Its rationale, per the RBI, is to "ensure better monitoring, unfettered supervisory access, and enhanced data security."[9] To comply with the circular, global firms must now reconfigure infrastructure by setting up India-specific data centers and introduce access controls that restrict foreign data processing. Additionally, they must ensure automated data purging protocols are in place to satisfy the 24-hour repatriation rule. This is because, notably, the RBI has not accepted storage in international cloud platforms, even with encryption, unless the physical servers are located in India and thus are under its legal jurisdiction. [10]

The requirements have led industry associations such as NASSCOM and the Payments Council of India to express concerns over cost burdens and the compliance load on smaller entities.Nevertheless, so far, the RBI has not shown willingness to dilute the rule. Thus, as of early 2025, it remains in force as a strict sectoral obligation. [11]

II. RBI Guidelines on Payment Aggregators and Tokenization

In addition to the 2018 data localization mandate, the Reserve Bank of India (**"RBI"**) has also introduced layered obligations regarding card data security and payment credential storage, which are particularly relevant for fintech firms and e-commerce platforms. These guidelines began with the issuance of the Guidelines on Regulation of Payment Aggregators and Payment Gateways in March 2020, under Section 18 of the Payment and Settlement Systems Act, 2007. The guidelines explicitly prohibit merchants and intermediaries from storing card credentials, other than the last four digits of the card number and the issuer's name, and even require Payment Aggregators (PAs) to purge such data if previously collected.[12]

The RBI has subsequently reinforced this requirement through the Circular on Card-on-File Tokenisation (CoFT) dated September 7, 2021. The circular permitted only card issuers and authorized card networks to tokenize and de-tokenize card data, mandating the deletion of stored raw credentials by all other parties by January 1, 2022.[13] Thus, as per the framework, tokens may be issued only with the customer's explicit consent and must be unique to a combination of card, token requestor, and merchant.

The regulatory rationale behind this circular centers on data minimization and enhanced protection against card-not-present (CNP) fraud. While the DPDPA sets broad obligations under Section 8 for security safeguards, it does not directly regulate the lifecycle of payment instruments. Thus, in order to combat this potential for fraud or other illicit activity, the RBI's guidelines operationalize data minimization and restrict storage to tokenized representations that are unusable if compromised.[14]

From an enforcement perspective, while the RBI issued several extensions to the compliance deadline, it has insisted on full compliance by January 1, 2022. Post-deadline, merchants and platforms that failed to comply faced the risk of having payment services revoked or audited.[15] This regime has resulted in significant opera-

9 Khaitan & Co., Data Localization Laws: India (2020).

10 Nishith Desai Assocs., India's Flourishing Fintech Flambeau (2025).

11 NASSCOM, Comments on Draft Rules under the Digital Personal Data Protection Act, 2023 6 (Mar. 5, 2025).

12 RBI, Guidelines on Regulation of Payment Aggregators and Payment Gateways, ¶¶ 10.4–10.6 (Mar. 17, 2020).

13 RBI, Circular on Card-on-File Tokenisation, Ref. No. CO.DPSS.POLC.No.S-1211/02-14-003/2021-22, ¶¶ 4–6 (Sept. 7, 2021).

14 Digital Personal Data Protection Act, No. 22 of 2023, § 8; Nishith Desai Assocs., India's Flourishing Fintech Flambeau 18 (2025).

15 RBI, Press Release: Extension of Timeline for Tokenisation Implementation, Dec. 23, 2021.

tional restructuring across the fintech ecosystem, especially for digital marketplaces, subscription services, and international platforms that relied on card-on-file models. Moreover, only regulated entities such as card networks, issuing banks, or RBI-authorized token requestors (TRs) may generate or access tokens, effectively centralizing token issuance under RBI oversight.[16] This has led to an elevated role of licensed TRs, who now must undergo stringent security audits and periodic compliance checks.

As a result of these requirements, many industry bodies such as the Internet and Mobile Association of India (IAMAI) have observed that while the RBI's tokenization framework is well-intentioned, it has led to market concentration around a few large card networks and slowed the onboarding of smaller merchants unfamiliar with the token infrastructure.[17] However, the RBI has shown no signs of reversing course, arguing that consumer trust and payment integrity outweigh short-term integration costs. Thus, fintech companies, especially those relying on recurring payments or international merchant of record (MoR) models, have had to retool backend systems, build token vault integrations, and reevaluate partnerships with acquiring banks and gateway providers. These changes exemplify the RBI's increasingly granular approach to digital payments regulation, moving beyond high-level oversight of settlement infrastructure to actively shaping how payment data is stored, tokenized, and accessed. By tightly controlling credential storage and centralizing token issuance through licensed intermediaries, the RBI has positioned itself not merely as a financial regulator but as a gatekeeper of digital trust architecture within India's BFSI sector.

III. IRDAI Data Storage Obligations in the Insurance Sector

In parallel to the RBI's localization mandates in the payments domain, the Insurance Regulatory and Development Authority of India (IRDAI) has also enforced its own data localization regime applicable to all insurers operating in the Indian market. This requirement is based on the IRDAI (Maintenance of Insurance Records) Regulations, 2015, which were issued under the IRDAI Act, 1999, and the Insurance Act, 1938.[18]

Take Regulation 3 of the 2015 framework which imposes a clear obligation in form of: "Every insurer shall maintain the records in physical or electronic form in India," covering all policyholder records, proposal forms, claim documentation, underwriting papers, and customer communication. [19] This mandate applies to both Indian and foreign insurers operating through branches or joint ventures, and no exemption is provided for storage on foreign servers, even when using reputable cloud providers.

Unlike the RBI's 2018 directive, which permits cross-border processing during settlement provided data is returned within 24 hours, the IRDAI's regime is more rigid, disallowing even transient overseas data storage. This regulatory stance reflects a broader supervisory philosophy, in which IRDAI has consistently framed its data rules as essential to ensure immediate access to records for inspection, dispute resolution, and fraud detection, especially in the event of natural disasters or legal disputes in Indian courts.[20]

Furthermore, the regulations require insurers to maintain records for a minimum of seven years from the date of the last transaction, with IRDAI officials entitled to inspect and audit such records at any time.[21] The

16 RBI, FAQs on Tokenisation (2022).

17 Internet & Mobile Ass'n of India (IAMAI), Comments to RBI on CoFT Guidelines (2022).

18 IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3, Gazette of India, No. IRDA/Reg/20/107/2015 (July 31, 2015).

19 ibid.

20 Khaitan & Co., Data Localization Laws: India 5 (2020).

21 IRDAI Regulations, supra note 38, Reg. 4(1).

obligation extends to reinsurers and third-party administrators (TPAs), who must likewise ensure localized storage of claim data and processing records related to Indian policies. In practical terms what means is the framework imposes infrastructure constraints, especially on global insurers that might otherwise centralize data storage across jurisdictions. As such this means many foreign insurers operating in India have been required to establish India-specific data lakes or private cloud deployments. Moreover even those relying on Software-as-a-Service (SaaS) claim-processing vendors must ensure that data is processed and retained entirely within India's borders.

The IRDAI has further supplemented the 2015 regulations with sectoral circulars emphasizing data availability and audit trails. For instance, a circular issued in 2017 reiterated that insurers must not outsource core record-keeping functions in a manner that impedes regulator access, noting that IRDAI's on-site inspections had uncovered lapses in this regard.[22] As, although the Digital Personal Data Protection Act, 2023 (DPDPA) permits cross-border transfers by default, subject to government-imposed restrictions under Section 16, the IRDAI's regulatory powers are expressly preserved. Section 3 of the DPDPA notes that the Act does not override laws made by competent sectoral regulators unless expressly repealed.[23]

Thus, broadly speaking this overlapping obligation means that insurers, unlike many other entities, face non-negotiable localization standards irrespective of whether their processing qualifies for cross-border transfer under general data protection law. As a result, compliance teams in the insurance sector must implement infrastructure segregation and bespoke contractual terms with IT vendors to ensure full alignment with IRDAI's requirements.

IV. CERT-In Cybersecurity Directions on Breach Reporting and System Logging

It is also important to consider that in addition to the sectoral data storage mandates from RBI and IRDAI, BFSI entities operating in India are subject to mandatory cybersecurity protocols issued by the Indian Computer Emergency Response Team (CERT-In) under the Information Technology Act, 2000. On April 28, 2022, CERT-In issued a set of directions under its statutory authority in Section 70B(6) of the IT Act, imposing new obligations on all "service providers, intermediaries, data centers, body corporates, and government organizations", a scope that clearly includes banks, NBFCs, insurance firms, and fintech platforms. [24]

The most critical requirement under the 2022 Directions is the six-hour breach notification rule, which compels covered entities to report specified categories of cybersecurity incidents to CERT-In within six hours of becoming aware of them.[25] These incidents include unauthorized access, malware attacks, data leaks, denial-of-service events, targeted scans, and identity theft, as defined in Annexure I of the Directions.[26] These were clarified through subsequent FAQs by CERT-In that the six-hour window begins from the point of detection, not from internal escalation or triage, which has placed significant pressure on BFSI organizations to modernize their monitoring and incident response pipelines. [27]

22 IRDAI Circular No. IRDA/INT/CIR/INS/193/08/2017, "Guidelines on Outsourcing of Activities by Insurance Companies" (Aug. 3, 2017).

23 Digital Personal Data Protection Act, 2023, § 3; NASSCOM, Comments on Draft DPDPA Rules 6 (2024).

24 Information Technology Act, No. 21 of 2000, § 70B(6).

25 Indian Computer Emergency Response Team, "Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000," para. 4(a) (Apr. 28, 2022).

26 Ibid.

27 CERT-In, "Frequently Asked Questions on Directions dated 28.04.2022," v.1.0, Q4 (May 2022).

Beyond breach reporting, the 2022 Directions introduced three additional technical obligations:

- **Log Retention**: All covered entities must retain logs of all ICT systems operating in India for a rolling period of 180 days, stored locally and made available to CERT-In upon request. [28]
- **Time Synchronization**: All systems must be synchronized with Network Time Protocol (NTP) servers of the National Informatics Centre (NIC) or those traceable to NIC/NPL (National Physical Laboratory) to ensure consistent event timestamps. [29]
- **Registration and Record-Keeping by Service Providers**: Cloud, VPN, and data center service providers are required to register user data and transaction records, including logs of all customers who use their infrastructure, and must maintain this information for at least five years. [30]

While these directives apply uniformly across sectors, their impact on the BFSI sector has been disproportionately high, especially for fintech companies relying on real-time data analytics, outsourced cloud security tools, or even globally distributed teams. For example, the six-hour incident reporting requirement is one of the shortest globally, significantly shorter than the 72-hour window under the EU's General Data Protection Regulation (GDPR). [31] These can create serious compliance challenges in cases where SOCs (Security Operations Centers) are outsourced or automated. Moreover, the Directions also mandate that any processing of personal data in India must leave sufficient forensic audit trails, and companies must ensure that their IT architectures are aligned with India's national security priorities. This obligation seems to dovetail with DPDPA's broader purpose limitation and storage limitation principles, but CERT-In's Directions carry independent enforcement authority under the IT Act and can result in separate fines or criminal liability for noncompliance. [32]

This prompted industry pushback, most notably through NASSCOM's public call for inputs requesting clarification or phase-wise implementation of the Directions. [33] However, MeitY largely stood firm: during a June 10, 2022, stakeholder meeting, it defended the stringent six-hour reporting requirement and refused to extend the timeline. [34]

Thus, it is important that BFSI companies must treat CERT-In's Directions not as advisory cybersecurity guidelines but as enforceable statutory obligations. While these obligations may overlap with RBI's cyber-resilience expectations, IRDAI's operational risk standards, and DPDPA's consent and breach protocols, it is important that firms be able to navigate the dense compliance web proactively through internal playbooks, training, and vendor negotiations to avoid sanctions.

28 CERT-In Directions, supra note 47, para. 4(g).

29 Ibid., para. 4(f).

30 Ibid., para. 5(a).

31 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).

32 Information Technology Act, 2000, §§ 66–72.

33 NASSCOM, Call for Inputs: CERT-In's Directions for a Safe and Trusted Internet, Community.nasscom.in (Apr. 28, 2022),

34 Saikrishna & Associates, CERT-In's Six-Hour Reporting Rule for Cyber Security Incidents: Statutory Interpretation and Analysis, Legal500.com (July 5, 2022),

V. Regulatory Treatment of Virtual Digital Assets (VDAs)

Although this paper does not focus on virtual digital assets (VDAs) or cryptocurrency-specific regulation, it is worth noting that India's financial regulatory environment has increasingly incorporated digital asset oversight through tax and reporting frameworks. The Finance Act, 2022 introduced a flat 30% tax on income from transfer of VDAs, alongside a 1% Tax Deducted at Source (TDS) on transfers exceeding INR 10,000.[35] Moreover, the Prevention of Money Laundering Act, 2002 was amended in March 2023 to bring crypto exchanges, wallet providers, and intermediaries under anti-money laundering (AML) obligations.[36]

Additionally, while there is no sector-specific localization or cybersecurity framework tailored for crypto under the RBI or CERT-In, regulated BFSI firms remain cautious about handling such data given evolving government attitudes and the absence of licensing. The Reserve Bank of India has consistently expressed scepticism toward cryptocurrencies, viewing them as a macroeconomic risk.[37]

35 Finance Act, No. 6 of 2022, § 115BBH, Gazette of India, Extraordinary, Part II, sec. 1 (Mar. 30, 2022).

36 Ministry of Finance, Notification No. SO 1072(E), Gazette of India (Mar. 7, 2023) (extending PMLA obligations to crypto intermediaries).

37 Reserve Bank of India, Financial Stability Report 92 (Dec. 2022).

Enforcement Landscape in India

India's data protection enforcement environment in the BFSI sector is characterized by complex web of multi-institutional oversight, involving both the newly created Data Protection Board of India (DPBI) under the Digital Personal Data Protection Act, 2023 (DPDPA), and sectoral regulators such as the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), and the Indian Computer Emergency Response Team (CERT-In). This overlapping regulatory structure creates a co-regulatory enforcement regime, in which fintech and financial entities must comply with general privacy laws as well as vertical mandates enforced by financial and cybersecurity regulator, and can difficult for firms to navigate.[1] However, this enforcement landscape should no longer be described only in forward-looking terms: the Board has already been formally established, even though substantive obligations under the DPDP framework are still coming into force in phases.[2]

Starting with the DPBI, which established under Chapter V of the DPDPA, is vested with broad enforcement powers, including the ability to inquire into breaches, direct remedial measures, impose monetary penalties, and conduct hearings following notices of violation.[3] For example, BFSI entities classified as Significant Data Fiduciaries under Section 10, the Board may impose additional obligations, such as the appointment of a Data Protection Officer, performance of periodic data audits, and conduct of Data Protection Impact Assessments (DPIAs). These obligations are layered over existing requirements from RBI, IRDAI, and CERT-In, increasing the compliance burden for affected firms.[4]

Moreover, the RBI, though not designated under the DPDPA, remains the de facto enforcer of payment data obligations in India. Since its 2018 localization directive, the RBI has routinely issued show-cause notices, onboarding restrictions, and operational suspensions against payment system operators failing to comply with its mandates. Notably, it blocked American Express, Mastercard, and Diners Club from onboarding new customers in India for more than a year due to non-compliance with local storage requirements.[5] The RBI also actively monitors implementation of tokenization standards, storage restrictions, and merchant compliance through inspections and compliance audits.[6]

Similarly, IRDAI also enforces its 2015 data localization regulations through regulatory inspections, requests for information, and licensing conditions. Violations may trigger penalties under Section 102 of the Insurance Act, 1938, or result in directives to cease certain practices.[7] Moreover, given the lack of clarity around cloud usage, IRDAI has continued to require Indian hosting of all policyholder records without exception, and has occasionally ordered insurers to migrate infrastructure away from third-country jurisdictions to remain compliant.[8] It is also important to note that IRDAI has extended the applicability of its information and cyber security guidelines to all insurance intermediaries with immediate effect, and it also issued a Circular

1 Digital Personal Data Protection Act, 2023, § 3.

2 (Ministry of Electronics and Information Technology Notification establishing the Data Protection Board of India, 13 Nov. 2025; Digital Personal Data Protection Rules, 2025).

3 Digital Personal Data Protection Act, 2023, §§ 27–33.

4 Vidhi Centre for Legal Policy, Submission on Draft Digital Personal Data Protection Rules, at 2–5 (2024).

5 Reserve Bank of India, Press Release, July 14, 2021.

6 Nishith Desai Associates, India's Flourishing Fintech Flambeau, at 18 (2025).

7 Insurance Act, No. 4 of 1938, § 102; IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3.

8 Khaitan & Co., Data Localization Laws: India, at 5 (2020),

on Cyber Incident or Crisis Preparedness in March 2025, thereby adding a more explicit cyber-resilience and crisis-readiness layer to insurance-sector compliance.[9]

Finally, the CERT-In, though primarily a cybersecurity agency, has also emerged as a powerful enforcement body under Section 70B of the Information Technology Act, 2000. Its 2022 Directions impose obligatory breach notifications within six hours, log retention mandates, and time synchronization requirements, with non-compliance punishable by fines or criminal prosecution under the IT Act.[10] Enforcement efforts include spot audits, summons, and mandatory compliance reports, especially for cloud providers and digital payments firms that fall within its broad definitional reach.[11]

The interplay between these agencies has given rise to what one may call a "stacked enforcement model." For example, a single incident of a payment data breach might require (1) breach notification to CERT-In within six hours, (2) disclosure to the RBI if payment system infrastructure is affected, (3) compliance checks by the DPBI for violation of general data processing principles under DPDPA, and (4) potential sector-specific remediation if insurance records are involved. This regulatory layering can produce not only operational friction, but also legal uncertainty due to the absence of clear delineation of jurisdictional boundaries.[12]

Moreover there a risk of "forum shopping" or "regulatory collision" between sectoral regulators and the DPBI. For instance, if a fintech firm complies with RBI storage mandates but violates DPDPA's consent or purpose limitation principles, questions arise as to which body has primacy in enforcement. While DPDPA attempts to resolve this by stating it is in addition to, not in derogation of, other laws,[13] practical conflicts may persist until detailed implementation rules or memoranda of understanding between regulators are adopted.[14]

Enforcement in India's BFSI data protection landscape is fragmented but intensive, with increased monitoring, licensing consequences, and multi-vector penalties becoming common. In order to stay on the right side of the law Fintech firms must develop compliance architectures that not only satisfy horizontal obligations under the DPDPA, but also adhere to vertical sectoral mandates from RBI, IRDAI, and CERT-In, while preparing for simultaneous scrutiny by multiple authorities.[15]

9 IRDAI, Guidelines on Information and Cyber Security; IRDAI, Circular on Cyber Incident or Crisis Preparedness, Mar. 2025

10 Indian Computer Emergency Response Team, "Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000," Apr. 28, 2022, ¶ 4,

11 Internet Society India & IIB, Briefing Note on CERT-In Directions, at 3–4 (2022),

12 Vidhi Centre for Legal Policy, Submission on Draft Digital Personal Data Protection Rules, at 6 (2024),

13 Digital Personal Data Protection Act, 2023, § 38.

14 Ibid.

15 Ibid.

GLBA and the Sectoral Framework for Financial Data in the U.S.

The United States overall adopts a more sectoral and federated approach to data privacy regulation which stands in contrast to India's more omnibus regime under the Digital Personal Data Protection Act, 2023. Nonetheless there are some federal laws that regulate BFSI industry. For example the primary federal statute governing personal financial data is the Gramm-Leach-Bliley Act of 1999 (GLBA), which establishes privacy obligations for financial institutions that offer consumers products or services such as loans, financial or investment advice, or insurance. GLBA is comprised of three key components: the Privacy Rule, the Safeguards Rule, and the Pretexting Rule.[1]

The Privacy Rule, implemented by federal banking agencies and the Federal Trade Commission (FTC), requires covered financial institutions to provide clear notices explaining their data collection and sharing practices. These notices must outline what categories of non-public personal information (NPI) the institution collects, how it uses and shares such information, and the consumer's right to opt out of certain types of third-party sharing.[2] While the notice and opt-out framework reflects an effort to secure consent, it is considerably weaker than India's DPDPA, which mandates opt-in consent by default.[3]

Moreover, the Safeguards Rule, enforced primarily by the FTC and other federal regulators such as the Office of the Comptroller of the Currency (OCC), requires financial institutions to develop, implement, and maintain a written information security program that contains administrative, technical, and physical safeguards appropriate to the size, complexity, and nature of the institution.[4]A major update to the Safeguards Rule took effect in June 2023 which introduced more granular requirements including encryption of customer data at rest and in transit, regular risk assessments, incident response planning, and designation of a qualified individual to oversee security operations.[5] The FTC's Safeguards Rule breach-notification requirement is now in force and requires covered financial institutions to notify the FTC as soon as possible, and no later than thirty days after discovery, of certain security breaches affecting at least 500 consumers[6]

Finally, the Pretexting Rule prohibits financial institutions and their affiliates from obtaining customer information through false pretences, including impersonation or deception. This is particularly relevant for preventing social engineering attacks in the financial sector and reflects a narrower but important focus on identity protection. Enforcement of the rule is carried out by the FTC and banking regulators under Section 523 of the GLBA, and institutions are expected to implement training and internal controls to detect and prevent such tactics.[7]

1 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018).

2 Privacy of Consumer Financial Information, 12 C.F.R. pt. 1016 (2023).

3 Digital Personal Data Protection Act, 2023, § 7.

4 Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2022).

5 FTC Final Rule, 86 Fed. Reg. 70302 (Dec. 9, 2021).

6 Federal Trade Commission, Safeguards Rule Notification Requirement Now in Effect (2024).

7 15 U.S.C. § 6821 (2018).

In addition to GLBA, they are many sector-specific statutes apply in niche areas. For example the Fair Credit Reporting Act (FCRA) regulates the use of consumer credit information, including rules for accuracy, disclosure, and dispute resolution for credit reporting agencies.[8] Likewise, the Right to Financial Privacy Act (RFPA) protects the confidentiality of financial records held by institutions from government access without customer consent or legal process.[9] The multiplicity of these statutes illustrate the fragmented and federated nature of the U.S. framework, in which different obligations arise depending on the type of data, the entity involved, and the purpose of use.

The U.S. approach though must also be understood to be deeply institutionalized as enforcement is dispersed across multiple agencies: the FTC, the OCC, the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), and state attorneys general all have overlapping jurisdiction depending on the type of institution and alleged violation. It also must be considered however that GLBA does not impose any data localization requirements or restrictions on cross-border data transfers, setting it apart from India's RBI mandate. Instead, financial institutions are expected to ensure security and accountability through contracts with third-party vendors, regardless of geographic storage location. The federal framework has also evolved in another important BFSI direction: the CFPB's Personal Financial Data Rights rule under section 1033 of the Dodd-Frank Act now stands as a major development in consumer financial data governance, although the CFPB states that its compliance dates were stayed by a federal court on 29 October 2025.[10]

Overall, while GLBA and related laws do offer baseline privacy protections, their opt-out model, lack of centralized enforcement, and sectoral fragmentation pose compliance challenges for FinTechs operating across multiple domains. These features contrast sharply with India's top-down structure, where sectoral rules supplement, rather than substitute, the general data protection law.

8 Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2023).

9 Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2023).

10 Consumer Financial Protection Bureau, Personal Financial Data Rights (updated Jan. 2026).

Cross-Border Data Transfers and Cloud Use in the U.S. BFSI Sector

The United States does not impose any formal data localization requirements for the financial services sector. This is because the default regulatory approach in the U.S. Favors cross-border data flows: regulated financial institutions are generally allowed to store and process data in foreign jurisdictions, provided they implement reasonable contractual safeguards and remain subject to oversight by their primary supervisory agencies. This is unlike India's regulatory regime, which includes explicit localization mandates and central government oversight of outbound data transfers under Section 16 of the Digital Personal Data Protection Act, 2023.[1]

Instead, under the Gramm-Leach-Bliley Act (GLBA), there is no statutory restriction on the geographic location of data storage. Rather, the Safeguards Rule requires financial institutions to implement administrative, technical, and physical protections when engaging service providers, including offshore vendors, to ensure that customer data remains secure regardless of where it is processed.[2] This means that institutions are expected to conduct due diligence, enter into binding contracts, and monitor vendors' compliance with applicable security standards. Thus, the onus of risk management is placed on the covered entity as opposed to the federal government.

The more accommodating stance toward international data transfer is echoed in official policy documents. For example, the U.S. Department of the Treasury, in its 2023 report on the future of financial infrastructure, reaffirmed its support for "cross-border data flows" as essential to financial innovation and global competitiveness, while noting that security and regulatory compliance must be preserved through risk-based governance rather than geographic restrictions.[3] This more open orientation is consistent with the U.S. approach in international forums like the G20 and OECD, where the U.S. has repeatedly opposed data localization mandates, arguing that they fragment the internet, raise compliance costs, and hinder trade.[4]

This position is supportive of U.S. financial institutions, especially FinTechs, which rely heavily on cloud-based infrastructure for core operations. That being said, federal regulators have recognized some risks and issued guidance accordingly. For example, in 2021, the Federal Financial Institutions Examination Council (FFIEC) issued a joint statement emphasizing the need for robust third-party risk management practices in cloud outsourcing, particularly with respect to data confidentiality, integrity, and availability.[5] Notably, this guidance does not prohibit the use of foreign cloud servers, provided institutions maintain effective controls and regulatory access, ensuring U.S. financial institutions are not adversely affected.

Moreover, even at the state level, there is similarly no prohibition on cloud use or cross-border data flows in the BFSI context. However, institutions may face additional obligations under privacy laws like the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), particularly for personal data not covered by GLBA.[6] These obligations may include consumer notice, deletion rights, and data minimization, which can affect how data is processed and shared across borders, even if not outright banning offshore storage, but vary greatly from state to state.

1 Digital Personal Data Protection Act, 2023, § 16.

2 Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2022).

3 U.S. Department of the Treasury, The Future of Money and Payments 25–26 (2023).

4 G7 Rejects Data Localization, Backs Cross-Border Digital Trade, Reuters (Apr. 28, 2021),

5 Federal Financial Institutions Examination Council (FFIEC), Joint Statement: Security in a Cloud Computing Environment (2021),

6 Cal. Civ. Code §§ 1798.100–1798.199 (2023).

Overall, the U.S. regime embodies a more open, flexible, and risk-based approach to international data transfer in the BFSI sector. While this flexibility allows for operational scalability and cost-efficiency, particularly for FinTechs operating in multiple jurisdictions, it does place greater responsibility on firms to navigate layered contractual, regulatory, and technical requirements. The U.S. trajectory, however, is no longer purely laissez-faire: consumer financial data access and transfer are now also being shaped by section 1033 rulemaking, even if the operative compliance timetable remains unsettled because of the stay.[7] When compared to India's sovereign, command-and-control approach, the U.S. model prioritizes industry autonomy and innovation, albeit at the cost of regulatory fragmentation and inconsistencies in consumer protection.

7 Consumer Financial Protection Bureau, Personal Financial Data Rights (updated Jan. 2026).

State-Level Privacy Laws and GLBA Exemptions

In keeping with the federated nature of the U.S. data protection framework, the Gramm-Leach-Bliley Act (GLBA) provides a federal baseline for the protection of consumer financial data but does not pre-empt state-level privacy legislation that regulates data outside its defined scope.[1] As a result, five U.S. states, most notably California, Virginia, Colorado, Connecticut, and Utah, have enacted comprehensive privacy laws that introduce new rights and obligations for businesses processing personal data. However, many other states have followed suit. In 2023, eight additional states enacted comprehensive consumer privacy laws: Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas. In 2024, seven more did so: Kentucky, Nebraska, New Hampshire, New Jersey, Maryland, Minnesota, and Rhode Island. Accordingly, by 2024 the number of states with comprehensive consumer privacy laws had reached at least nineteen.[2] For financial institutions and fintech firms, these laws may present a layered compliance challenge: while most exempt data collected "pursuant to" GLBA, they continue to apply to other categories of data processed in the course of business, including employee records, business partner information, and behavioral or marketing data. This complexity can have direct consequences for firms seeking to operate at scale across multiple jurisdictions or offer ancillary services beyond traditional banking or insurance.

California Consumer Privacy Act (CCPA/CPRA)

California remains the most significant subnational privacy regulator in the United States. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), includes an exemption for "personal information collected, processed, sold, or disclosed pursuant to the federal GLBA."[3] However, the CPRA's implementing regulations as interpreted by the California Privacy Protection Agency (CPPA), clarify that this exemption is transaction-specific, not entity-wide. That means that only those data elements collected in direct connection with providing a financial product or service to a consumer, such as loan application data or account credentials, are excluded. Information collected outside that transaction, such as employee monitoring logs, HR records, third-party vendor contacts, geolocation data, or clickstream analytics, remains subject to CPRA rules.

For fintech firms, this partial exemption can create some operational friction. For instance, a digital lending platform may be exempt for its consumer credit underwriting data but not for behavioral analytics used to refine marketing or customer engagement strategies. Additionally, the CPRA also introduces specific obligations such as providing granular privacy notices[4] which enable data subject access, deletion, and correction requests,[5] and executing data processing agreements with service providers.[6] Financial institutions must therefore adopt segmented compliance architectures to maintain a defensible position under both GLBA and CPRA.

1 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018).

2 National Conference of State Legislatures, Summary 2023 Consumer Data Privacy Legislation; National Conference of State Legislatures, Summary 2024 Consumer Data Privacy Legislation.

3 Cal. Civ. Code § 1798.145(e) (2023).

4 Id. § 1798.100(a).

5 Id. §§ 1798.105–1798.106.

6 Id. § 1798.140(v).

Notably, the CPRA also created a new regulatory agency, the CPPA, which is tasked with rulemaking and enforcement. This introduces the potential for dual enforcement in California: while the Federal Trade Commission (FTC) remains the primary federal enforcer for unfair or deceptive practices under Section 5 of the FTC Act, the CPPA has independent authority to investigate and fine entities under the state's privacy regime.

Other State-Level Laws: Virginia, Colorado, Connecticut, Utah

Outside California, four other states have passed broadly applicable privacy legislation: Virginia's Consumer Data Protection Act (CDPA), Colorado's Privacy Act (CPA), Connecticut's Data Privacy Act (CTDPA), and Utah's Consumer Privacy Act (UCPA). Each of these statutes contains exemptions for GLBA-covered data, but the scope of these exemptions, and thus the associated compliance burdens, varies materially.

For example, Virginia's CDPA exempts "financial institutions or data subject to Title V of the GLBA."[7] Colorado's CPA applies the exemption to "information subject to Title V" rather than the institution itself.[8] This technical distinction in Colorado's CPA means that even GLBA-regulated financial entities may fall under its scope if they process data not covered by Title V, such as employee records, commercial customer data, or marketing profiles. Additionally, these state laws often impose opt-out rights for profiling, targeted advertising, and the sale of personal data, areas typically not addressed by GLBA.

Moreover, enforcement authority in these states rests primarily with state attorneys general (AGs), many of whom have taken aggressive stances on consumer protection. For example, the Colorado Attorney General's Office has issued non-binding interpretive guidance emphasizing the narrow nature of the GLBA exemption and encouraging financial firms to develop "data purpose maps" to clearly delineate covered versus non-covered data processing activities. Connecticut's CTDPA similarly encourages firms to implement internal governance structures capable of honoring opt-out rights and demonstrating "data minimization" across systems not explicitly governed by federal law.[9] In contrast, Utah's Consumer Privacy Act (UCPA) adopts a more lenient posture: it exempts both financial institutions and Title V-covered data, grants no rulemaking authority to the AG, and generally avoids prescriptive compliance burdens, showing how varied the regulatory regimes are overall.[10]

For fintech firms specifically, especially those involved in insurance aggregation, digital wallets, investment platforms, or peer-to-peer lending, these obligations present non-trivial compliance costs. Unlike legacy financial institutions that may confine operations within GLBA-covered domains, FinTechs often operate across verticals, deploying sophisticated behavioral data models, AI-based decision-making, or social media integrations that fall squarely within the scope of many of these state laws.

7 Va. Code Ann. § 59.1–581.5(A)(1) (2023).

8 Colo. Rev. Stat. § 6-1-1304(2)(j) (2023).

9 Conn. Gen. Stat. §§ 42-515 to 42-525 (2023).

10 Utah Code Ann. §§ 13-61-101 to 13-61-404 (West 2023).

GLBA-Exempt Data ≠ GLBA-Exempt Entity

A key point of confusion, frequently misunderstood by fintech startups, is that the state-level GLBA exemption is based on data, not entities. This means that a company cannot claim blanket exemption simply because it is registered with a financial regulator. For example, a payments app that collects user behaviour data for churn analysis, location tracking, or referral programs must treat that data as subject to state privacy law unless it is demonstrably collected "pursuant to" a GLBA-covered transaction. Some industry associations may favor broader uniformity and have urged states to adopt broader pre-emption clauses; however, these efforts have not yet been successful. Instead, firms must rely on internal classification frameworks to determine whether specific data assets fall inside or outside the scope of GLBA.

Summary and Strategic Considerations

In practice, financial entities operating across multiple states must undertake detailed regulatory mapping exercises to manage risk. These may include:

- Segregated storage systems for GLBA-covered and non-GLBA data.
- Tiered privacy notices for customer versus non-customer data subjects.
- State-specific opt-out mechanisms for behavioral advertising and data sale.
- Workforce privacy protocols (for employee, contractor, or applicant data).
- Modular service provider contracts to ensure downstream compliance.

For fintech firms planning to expand into India, this regulatory fragmentation contrasts sharply with India's centralized and co-regulatory model, where cross-sectoral data rules are typically issued at the Union level, with limited subnational variation. While India imposes localization and breach reporting burdens through its sectoral regulators, U.S. firms face a growing patchwork of consumer rights and enforcement mechanisms that differ substantially by state and type of data. As the number of state privacy laws expands, with Texas, Oregon, and others implementing new laws in 2024 and 2025, the pressure to harmonize compliance frameworks will intensify.[11] Financial firms must thus be prepared for increasing complexity, especially as enforcement shifts toward litigation in states like California and Colorado, coupled with the practical difficulty it is no longer simply whether California remains the dominant outlier, but whether non-GLBA data can be mapped, segmented, and governed across an expanding and increasingly heterogeneous group of state privacy regimes.[12]

11 Tex. Bus. & Com. Code Ann. §§ 541.001–541.302 (West 2024).

12 National Conference of State Legislatures, Summary 2024 Consumer Data Privacy Legislation.

U.S. Regulatory Approach to Cryptocurrencies and Digital Assets

While the core of this paper centers on conventional financial data regulation in the BFSI sector, the treatment of cryptocurrencies and digital assets in the U.S. remains a significant, yet distinct, legal topic. Federal oversight of crypto assets remains fragmented, with the Securities and Exchange Commission (SEC) asserting jurisdiction where crypto tokens qualify as securities under the Howey test.[1] Meanwhile, the Commodity Futures Trading Commission (CFTC) treats Bitcoin and Ethereum as commodities.[2]

The Financial Crimes Enforcement Network (FinCEN) also plays a key role by subjecting crypto exchanges and wallet providers to Bank Secrecy Act compliance, including Know-Your-Customer (KYC) and anti-money laundering (AML) controls.[3] Although no federal law imposes data localization or cross-border restrictions on crypto-related data, state laws such as New York's BitLicense framework create indirect compliance burdens for crypto-fintech interfaces.[4] This paper does not focus on the legal treatment of crypto-assets or blockchain infrastructure, but a possible avenue for future research could explore how overlapping crypto regulations intersect with mainstream financial data governance.

1 SEC v. Ripple Labs Inc., No. 20-cv-10832 (S.D.N.Y. 2023).

2 See CFTC, In re Coinflip, Inc., CFTC No. 15-29 (Sept. 17, 2015).

3 31 C.F.R. § 1010.100(ff).

4 23 NYCRR 200.

Cybersecurity Regulations – NYDFS and NAIC Model

In line with the principle of federalism, while the federal GLBA Safeguards Rule provides baseline obligations for data security in the financial sector, a number of U.S. states have adopted more prescriptive cybersecurity requirements. The most prominent of these states is New York, which has: (i) cybersecurity regulations for financial services companies under 23 N.Y.C.R.R. Part 500, administered by the New York Department of Financial Services (NYDFS), and (ii) the Insurance Data Security Model Law developed by the National Association of Insurance Commissioners (NAIC), which has been adopted by over 26 states as of 2025.[1] These frameworks impose more concrete and risk-based security obligations that are highly relevant to fintech firms and BFSI entities operating in or regulated by U.S. states.

NYDFS Cybersecurity Regulations: 23 N.Y.C.R.R. Part 500

New York's cybersecurity rules, first effective in March 2017 and significantly updated in 2023, apply to any entity licensed, registered, or otherwise authorized by the NYDFS, including state-chartered banks, insurance companies, mortgage lenders, and money transmitters. The regulations mandate the implementation of a comprehensive cybersecurity program based on the entity's risk assessment, covering governance, technical controls, incident response, and third-party risk management.[2]

Key requirements include:

- **Annual Risk Assessments**: Companies must conduct and document periodic risk assessments to inform cybersecurity program design.[3]
- **CISO Appointment**: Covered entities must designate a qualified Chief Information Security Officer responsible for overseeing cybersecurity and reporting to the board at least annually.[4]
- **Multi-Factor Authentication (MFA)**: MFA is required for all external access and for internal access to sensitive systems unless the CISO approves reasonably equivalent controls.[5]
- **24-Hour Breach Notification**: Covered entities must notify NYDFS within 24 hours of a "cybersecurity event" that impacts material operations or requires notice to another regulator or government body.[6]
- **Third-Party Service Provider Oversight**: Firms must implement policies ensuring that external vendors meet minimum security standards, especially when handling non-public personal information (NPI).[7]

Amendments introduced in 2023 tiered compliance standards based on company size and risk profile. This is seen in DFS's own compliance materials now identify staggered implementation milestones extending

1 Nat'l Ass'n of Ins. Comm'rs, Insurance Data Security Model Law (#668), Implementation Status Brief (May 2025).
2 N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. § 500.2–500.3 (2023).
3 Id. § 500.9.
4 Id. § 500.4.
5 Id. § 500.12.
6 Id. § 500.17(a).
7 Id. § 500.11.

through 2025, including access-privilege review and asset-inventory requirements.[8] Thus, Class A entities, those with over $20 million in gross revenue and more than 2,000 employees, must conduct independent audits, implement endpoint detection tools, and segregate user access rights based on job function.[9] Fintech companies operating in New York or seeking money transmitter or lending licenses must account for these rules even if they fall below the Class A threshold, as baseline obligations still apply to all covered entities. Enforcement has been aggressive; for example, NYDFS imposed an $18 million penalty on EyeMed Vision Care in 2023 for failing to maintain adequate email protections and access controls, even though the underlying breach stemmed from phishing and in October 2025 announced that it had secured more than $19 million in penalties from eight auto insurance companies for violations of its cybersecurity regulation after breaches exposed New Yorkers' personal data. [10] [11]

NAIC Insurance Data Security Model Law (MDL-668)

In addition to the NYDFS regime, the NAIC developed its Insurance Data Security Model Law (Model #668) in 2017, which has since been adopted by over 20 states, including Michigan, Ohio, South Carolina, and Virginia. This law mandates cybersecurity programs, risk assessments, and breach notification standards for licensed insurers and insurance-related entities.[12]

Although modelled loosely on NYDFS rules, the NAIC law includes important distinctions:

- Breach Notification Timeline: Licensees must notify state insurance regulators within three business days of a cybersecurity event that has a reasonable likelihood of harming consumers.[13]
- Oversight of Affiliates and Vendors: Licensees are responsible for ensuring that affiliates and third-party service providers maintain comparable data security programs.[14]
- Annual Certification: Licensees must annually certify compliance with the law and retain supporting documentation for at least five years.[15]

As a result, many FinTechs entering the U.S. insurance sector as administrators, Insurtech firms, or digital brokers may be indirectly subject to these requirements through licensing arrangements or partnerships with regulated insurers. For example, a licensed digital Managing General Agent (MGA) would be required to submit annual compliance statements and adopt a formal incident response plan, even if it outsources technology development to a third-party vendor.[16]

8 New York Department of Financial Services, Cybersecurity: Part 500 Requirement Checklist for Regulated Entities with Limited Exemptions

9 N.Y. Dep't of Fin. Servs., Second Amendment to Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. § 500 (effective Nov. 1, 2023).

10 NYDFS Consent Order, Matter of EyeMed Vision Care LLC (2023).

11 New York Department of Financial Services, Superintendent Harris Secures More than $19 Million from Auto Insurance Companies for Cybersecurity Violations (14 Oct. 2025)

12 NAIC MDL-668, Insurance Data Security Model Law, § 3–7 (2017).

13 Id. § 6.

14 Id. § 7.

15 Id. § 4(H).

16 Id. §§ 4–5.

Combined Compliance Impact

Overall, the dual landscape of NYDFS and NAIC rules means that FinTechs working in both banking and insurance spaces may be subject to overlapping but distinct cybersecurity requirements. Although federal rules under the GLBA Safeguards are relatively high-level and principle-based, these state-derived frameworks introduce operational specificity that requires tailored controls. Notably, the requirement to report breaches within 24 hours (NYDFS) or three business days (NAIC) is stricter than most federal timelines, increasing the pressure on incident detection and escalation systems.[17]

Firms with cloud-heavy architectures, distributed teams, and reliance on third-party vendors must invest in robust vendor oversight mechanisms, log aggregation tools, endpoint detection and response (EDR) solutions, and MFA enforcement across platforms. Moreover, compliance is not merely a checkbox exercise: both NYDFS and NAIC regulators have demonstrated an increasing willingness to issue fines, require remediation plans, and publicly name non-compliant entities, which can impact investor confidence and consumer trust.

Compared to India's regime, where cybersecurity rules such as CERT-In directions apply nationally and uniformly, U.S. FinTechs must track and comply with divergent state laws, with varying thresholds, requirements, and regulators. This more decentralized model can complicate cross-border service delivery and even internal compliance harmonization for firms operating in both India and the U.S.

17 Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2022).

Enforcement and Regulatory Agencies

The United States enforces data protection and cybersecurity in the BFSI sector through a complex network of federal and state regulators, with overlapping jurisdiction across privacy, consumer protection, and financial regulation. Unlike India's co-regulatory model, which is anchored in statutory authorities such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI), and CERT-In, the U.S. lacks a single dedicated data protection authority. Instead, enforcement responsibilities are dispersed among agencies like the Federal Trade Commission (FTC), financial regulators such as the Office of the Comptroller of the Currency (OCC), Federal Reserve Board, and Federal Deposit Insurance Corporation (FDIC), as well as state attorneys general and specialized regulators such as the New York Department of Financial Services (NYDFS).

Federal Trade Commission – Section 5 Enforcement

The FTC remains the most prominent federal enforcer of consumer privacy and data security through its authority under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices."[1] While the FTC does not have rulemaking power to create a binding privacy code, it has developed a robust common law framework based on companies' failure to adhere to their stated data protection practices or implement reasonable safeguards. That role is operationally significant for BFSI actors because the FTC is now not only an ex post unfairness enforcer, but also the recipient of mandatory breach notifications under the amended Safeguards Rule when qualifying incidents affect 500 or more consumers.[2]

In the BFSI context, the FTC enforces the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and Privacy Rule against non-bank financial institutions, including payday lenders, mortgage brokers, FinTechs, and credit reporting services. Violations may result in multi-million dollar settlements, mandated audits, and long-term consent orders. For example, in 2023, the FTC fined a fintech firm $3.5 million for failing to encrypt user data and misrepresenting its security practices in violation of both GLBA and Section 5.[3]

The FTC has also begun targeting lax vendor oversight and data retention practices, areas increasingly important for fintech startups that rely on cloud-based services and AI-driven data analytics. A notable trend is the Commission's increasing focus on algorithmic accountability and data minimization, both of which intersect with emerging fintech risk models.

Federal Bank Regulators – OCC, Fed, and FDIC

For banks and savings institutions, primary supervisory authority lies with the OCC (for national banks), the Federal Reserve Board (for bank holding companies and state-chartered member banks), and the FDIC (for state-chartered non-member banks). Each regulator enforces data protection and cybersecurity obligations under the GLBA Interagency Guidelines Establishing Information Security Standards.[4]

1 15 U.S.C. § 45(a)(1) (2023).

2 Federal Trade Commission, Safeguards Rule Notification Requirement Now in Effect (2024).

3 Federal Trade Commission, "Fintech Firm to Pay $3.5 Million for Security Failures," Press Release (Mar. 15, 2023).

4 Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001).

These guidelines, adopted by all three regulators, require institutions to:

- Develop and maintain a written Information Security Program (ISP);
- Conduct risk assessments and adjust controls accordingly;
- Oversee service providers and ensure they maintain adequate protections;
- Train employees on security and privacy best practices;
- Report material cybersecurity incidents to the regulator and impacted customers.[5]

These agencies have issued guidance clarifying that third-party cloud vendors and fintech partners must be integrated into banks' security programs. For example, OCC Bulletin 2021-40 emphasized that banks remain responsible for ensuring third-party providers comply with risk management expectations, even when critical functions like KYC verification, API banking, or fraud detection are outsourced.[6] Thus, while enforcement actions by federal bank regulators are typically non-public, the agencies retain the power to impose civil money penalties, restrict new activities, or issue cease-and-desist orders for institutions failing to adequately secure customer data.

State Attorneys General and Sectoral Regulators

State attorneys general (AGs) also play a significant role in enforcing data protection rules, particularly under state consumer protection laws and state-specific privacy frameworks such as the California Consumer Privacy Act (CCPA) and its 2020 amendment, the California Privacy Rights Act (CPRA). Under CCPA/CPRA, the California AG (and now the California Privacy Protection Agency) may initiate investigations and levy penalties for unauthorized data sharing, security breaches, or failure to honor consumer rights, even where the data in question is "non-public personal information" exempt under GLBA.[7]

Other states, like Massachusetts and Illinois, have similarly empowered AGs to bring enforcement actions for data breaches or deceptive practices. For instance, in 2024, a coalition of AGs from New York, Illinois, and Washington launched a joint investigation into a national payment platform's use of facial recognition data in fraud prevention, arguing that the company failed to provide adequate disclosures or opt-outs under respective biometric privacy laws.[8] Moreover, separately, the NYDFS continues to aggressively enforce its cybersecurity regulations, issuing consent orders, monetary penalties, and mandated remediation programs. Its enforcement powers go beyond GLBA, including the ability to revoke licenses or restrict operations. In 2023 alone, NYDFS levied more than $40 million in cybersecurity-related fines across insurance and fintech licensees.[9]

Thus, the American approach to data protection enforcement in the BFSI sector is highly decentralized, sectorally fragmented, and enforcement driven. Rather than relying on a unified statutory regime or centralized data protection authority, as seen in India's co-regulatory framework, the U.S. relies on overlapping

5 Federal Financial Institutions Examination Council (FFIEC), IT Examination Handbook: Information Security (Nov. 2016).

6 Office of the Comptroller of the Currency, Bulletin 2021-40: Third-Party Relationships: Risk Management – FAQs to Supplement OCC Bulletin 2013-29 (Aug. 13, 2021).

7 Cal. Civ. Code § 1798.199.90 (2023) (authorizing CPPA enforcement); § 1798.155 (authorizing AG enforcement).

8 Office of the New York Attorney General, "AG James Leads Multistate Investigation into Facial Recognition Use by Payment App," Press Release (Apr. 3, 2024).

9 New York State Department of Financial Services, "Superintendent Harris Announces Over $40 Million in Cybersecurity Penalties in 2023," Press Release (Dec. 20, 2023).

mandates from multiple federal and state actors, each applying distinct substantive standards and remedies. This creates a dynamic but often unpredictable compliance landscape, especially for fintech firms operating across institutional categories or state lines. Enforcement emphasis tends to fall on post-incident accountability, vendor oversight, and procedural fairness, with limited room for ex ante licensing or preventive supervision. As a result, firms must build proactive governance architectures capable of navigating not just multiple regulators, but multiple conceptions of data risk, consumer harm, and institutional responsibility. In contrast to India's top-down regulatory coherence, the U.S. model offers operational flexibility and market responsiveness, yet at the cost of regulatory certainty, uniformity, and systemic clarity.

Navigating Regulatory Fragmentation and Compliance Overlap Across India and the United States / Comparative Operational Challenges for Cross-Border FinTechs

Fintech firms operating across India and the United States must navigate a uniquely complex cross-jurisdictional compliance landscape, marked by divergent legal philosophies, regulatory structures, and enforcement cultures. As detailed in Part I, India's data protection regime in the BFSI sector is vertically layered and co-regulatory in nature. Entities must simultaneously comply with the Digital Personal Data Protection Act, 2023 (**"DPDPA"**), RBI's 2018 payment localization circular, the IRDAI (Maintenance of Insurance Records) Regulations, 2015, and CERT-In's 2022 cybersecurity directions, all of which impose overlapping but non-identical obligations on data storage, breach reporting, and information security. Sectoral supervision continues even after the DPDPA's enactment, as the statute explicitly preserves the authority of financial regulators.[1] All of which sharpened rather than narrowed: India's movement since the original DPDP draft has come primarily through central rulemaking and institutional build-out under the DPDP framework, whereas the United States has continued to expand laterally through state privacy proliferation and agency-specific BFSI data and cybersecurity rules. [2]

This layered approach stands in sharp contrast to the more decentralized and sectoral structure of U.S. law, described in Part II. There, the Gramm-Leach-Bliley Act (**"GLBA"**) governs financial privacy and security through its Safeguards Rule and Privacy Rule, enforced primarily by the Federal Trade Commission (**"FTC"**) and prudential regulators such as the OCC and the Federal Reserve.[3] While state laws such as the California Consumer Privacy Act (**"CCPA"**) and the Virginia Consumer Data Protection Act (**"VCDPA"**) increasingly play a role, the GLBA continues to serve as the cornerstone for data protection in the BFSI sector, pre-empting many, but not all, state obligations for covered entities.[4]

Thus for U.S.-based fintech firms seeking to expand into India, this divergence in regulatory structure introduces high operational complexity. Whereas U.S. firms may be able to take a uniform national approach with limited state-level variation, Indian compliance requires disaggregation by regulatory function. A digital lender, for example, must comply with the DPDPA's notice and consent requirements,[5] localize all loan application and disbursal data under RBI guidelines,[6] and report breaches within six hours to CERT-In.[7] This imposes significantly greater planning and infrastructure costs compared to the U.S., where breach timelines typically range from 72 hours to 30 days.[8]

1 Digital Personal Data Protection Act, No. 22 of 2023, § 1(5); Reserve Bank of India, Circular DPSS.CO.OD No.2785/06.08.005/2017-18 (Apr. 6, 2018); Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, Reg. 3; Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), para. 4.

2 Digital Personal Data Protection Rules, 2025; National Conference of State Legislatures, Summary 2024 Consumer Data Privacy Legislation)."

3 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809; 16 C.F.R. Part 314.

4 Cal. Civ. Code §§ 1798.145(e); Va. Code Ann. § 59.1-581(A).

5 DPDPA § 6.

6 RBI Circular DPSS.CO.OD No.2785/06.08.005/2017-18 (Apr. 6, 2018).

7 CERT-In Directions, Apr. 28, 2022, para. 4.

8 23 N.Y.C.R.R. § 500.17(a); FTC v. Equifax Inc., No. 1:19-cv-03297 (N.D. Ga. 2019).

Moreover, the enforcement architecture compounds this complexity. In India, the newly constituted Data Protection Board operates alongside financial regulators, with each able to initiate proceedings or impose penalties for non-compliance.[9] In the U.S., however, enforcement is largely centralized within the FTC with respect to general consumer data, and GLBA-specific oversight is handled by bank regulators. This results in a more predictable, if still fragmented, enforcement pathway in the United States.

Importantly, these differences have strategic implications for resource allocation and legal operations. Indian regulations require granular technical and legal adaptations, such as separating financial transaction data subject to RBI localization from other personal data that may be stored or processed abroad under DPDPA's cross-border transfer provisions.[10] U.S. fintech firms must prepare for higher compliance overheads when entering India, particularly around data localization, breach reporting, and partnership structuring (e.g., token service providers).

Mid-sized fintech companies are especially vulnerable, as they often lack the scale to maintain separate compliance teams for each jurisdiction. Without local legal counsel and technical compliance partners, they risk regulatory exposure. India's ongoing rulemaking, especially around "significant data fiduciary" thresholds, currently under draft consideration by the Ministry of Electronics and Information Technology, further complicates long-term compliance planning.[11]

Ultimately, regulatory fragmentation is more than an administrative burden—it also shapes product design, cross-border architecture, and market viability. A comparative awareness of these differences is essential for fintech firms planning expansion across both jurisdictions.

9 DPDPA §§ 27–33.

10 DPDPA § 16.

11 Nishith Desai Associates, Fintech Compendium (2025), at 14–16.

Infrastructure and Data Localization Readiness

One of the most significant operational and legal burdens for U.S.-based fintech firms expanding into India is the infrastructure investment required to comply with India's data localization regime. Unlike the United States, where data localization is not mandated at the federal level and firms retain broad flexibility to use global cloud infrastructure, India has adopted a stringent localization-first policy in the financial sector through layered regulations issued by the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Indian Computer Emergency Response Team (CERT-In), all operating in parallel with the general-purpose Digital Personal Data Protection Act, 2023 (DPDPA).[1]

To better understand the difficulties, consider the previously discussed RBI's 2018 directive on "Storage of Payment System Data" which remains the cornerstone of India's financial localization mandate. It requires all payment system providers, defined broadly to include card networks, digital wallets, payment aggregators, and banks, to ensure that "the entire data relating to payment systems operated by them are stored in a system only in India," covering transaction details, customer data, instructions, and processing logs. The 2019 clarification further narrowed any flexibility by allowing limited cross-border processing only for settlement purposes, with a mandatory 24-hour repatriation and deletion requirement for foreign-hosted data.[2] This has led to compliance deadlines, freezes on onboarding non-compliant foreign card networks, and costly re-architecture for foreign players.[3]

Moreover, compounding these obligations, RBI's 2020 Guidelines on Payment Aggregators and Payment Gateways prohibit the storage of card credentials except for truncated card numbers and require FinTechs to adopt tokenization solutions exclusively through licensed networks or token requestors.[4] These rules culminated in the January 2022 purge deadline following the RBI's 2021 Circular on Card-on-File Tokenisation, which banned merchants and intermediaries from storing raw card data unless tokenized by an authorized party. [5]

Even in the insurance sector, IRDAI imposes its own localization requirement through the IRDAI (Maintenance of Insurance Records) Regulations, 2015, which mandate that all insurance policyholder records, claims, underwriting documents, and communications be stored exclusively in India without exemption.[6]Moreover, unlike DPDPA, which allows cross-border transfers subject to government approval under Section 16, IRDAI has not offered any waiver or interoperability mechanism for global cloud infrastructure.[7]

Furthermore, CERT-In's 2022 Directions apply horizontally to "service providers, intermediaries, data centres, body corporates and Government organisations," and effectively require that system logs be retained within India for a minimum of 180 days, and be available to CERT-In on demand.[8] This requirement reinforces India's architectural demand for localized data retention beyond the application layer.

1 Digital Personal Data Protection Act, 2023, § 3, Gazette of India, Ministry of Law and Justice (Aug. 11, 2023),

2 Reserve Bank of India, Storage of Payment System Data, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-18 (Apr. 6, 2018),

3 Insurance Regulatory and Development Authority of India, IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3, Gazette of India (Oct. 5, 2015),

4 Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-section (6) of Section 70B of the IT Act, 2000, Ministry of Electronics & IT (Apr. 28, 2022), para 4,

5 Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, (Mar. 17, 2020), ¶ 10.4,

6 Insurance Regulatory and Development Authority of India, IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3, Gazette of India (Oct. 5, 2015),

7 Khaitan & Co., Data Localization Laws: India (2020),

8 CERT-In Directions, supra note 136, para 4(g).

Thus, from a strategic standpoint, this localization imperative results in duplicative infrastructure, segmented cloud instances, and specialized engineering teams focused on jurisdiction-specific deployments. It undermines economies of scale and drives up compliance costs. For example, a U.S. fintech company offering AI-driven credit scoring or algorithmic trading would likely have to train its models on India-resident data using segregated compute resources, thereby losing the benefit of integrated learning systems and scalable infrastructure.

In contrast, the United States imposes no comparable localization mandate in the BFSI sector. The Gramm-Leach-Bliley Act (GLBA) sets forth security obligations under its Safeguards Rule and requires notice and consent for information sharing, but permits firms to store and process data globally as long as consumer privacy and security are maintained.[9] Likewise, sectoral regulators such as the Federal Reserve, OCC, and FDIC do not impose geographic storage requirements. Even in cybersecurity regulation, neither the NYDFS Part 500 rule nor the NAIC Insurance Data Security Model Law contains localization language.[10]

Thus, U.S.-based fintech firms face an asymmetry: operational freedom at home versus hyper-localized infrastructure demands in India. While cloud providers like AWS, Azure, and GCP offer India-based hosting and compliance tools, the onus remains on FinTechs to re-architect systems, isolate data flows, and prepare for audits.[11] As infrastructure bifurcation raises latency and user experience concerns, while also complicating vendor management when services like fraud detection or analytics aren't India-localized.[12] Many firms respond by building India-specific compliance and engineering teams, which increases costs and slows product rollout.[13]

These challenges directly shape capital allocation, whether to enter India at all, how to phase expansion, and whether to partner with local entities that already meet regulatory standards. For startups without dedicated compliance budgets, localization can be a de facto barrier to entry.[14] For well-resourced firms, however, it may serve as a trust-building advantage and strategic differentiator in accessing India's expanding digital economy.[15] Ultimately, while framed as "data sovereignty," localization effectively restructures the fintech value chain.[16]

9 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809.

10 New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500,

11 Nishith Desai Associates, Data Localization in India: Regulatory Landscape and Industry Implications, at 9–12 (2023),

12 NASSCOM & Data Security Council of India (DSCI), Building a Resilient and Trusted Digital India, at 17 (2023),

13 Boston Consulting Group (BCG) & FICCI, Unlocking the Potential of India's Digital Economy, at 26 (2024)

14 Carnegie India, The Costs of Data Localization for Startups (2023),

15 EY & FICCI, The Role of FinTech in Building Viksit Bharat, at 12 (2025),

16 Ministry of Electronics and Information Technology (MeitY), Explanatory Note on DPDPA Implementation Framework, at 14 (2024),

Risk Management and Incident Response

Fintech firms and other BFSI sector actors in both the United States and India would do well to have effective risk management and cybersecurity incident response protocols. Yet it is important to consider the regulatory expectations and operational norms in each jurisdiction diverge significantly. In particular, the U.S.-based fintech firms that plan on expanding into the Indian market would do well to recalibrate their risk assessment frameworks in India, due to its uniquely stringent breach notification requirements and evolving definitions of security incidents.

This is seen in the fact that in India, the key regulatory touchstone for cybersecurity is the Directions issued by the Indian Computer Emergency Response Team (CERT-In) under Section 70B of the Information Technology Act, 2000.[1] These April 2022 CERT-In Directions impose a six-hour breach notification mandate, measured from the time of detection rather than the point of internal reporting escalation.[2] This requirement applies broadly to entities offering "essential services," which includes most BFSI sector actors such as banks, non-banking financial companies (NBFCs), insurance firms, intermediaries, and cloud infrastructure providers. As such, the range of reportable incidents is extensive, encompassing unauthorized access, phishing attacks, data breaches, denial-of-service events, and ransomware incursions.[3]

Additionally, the CERT-In Directions mandate:

- Retention of system logs within India for 180 days, available to CERT-In on request.[4]
- Time synchronization of system clocks to the National Informatics Centre (NIC) or NPL-certified NTP servers.[5]
- Mandatory registration and record-keeping obligations for data center, VPN, and cloud service providers, including Know Your Customer (KYC) information for all users.[6]

These obligations would particularly impact foreign FinTechs offering services in India, especially those relying on global security monitoring tools or cloud-based log management systems, as they would be required to engage in substantial reengineering of their services in order to comply. As such, India's six-hour standard is among the most aggressive globally and contrasts sharply with norms in the U.S. and EU, where breach reporting thresholds are more flexible and often linked to actual harm to consumers.[7]

In the U.S., regulators instead tend to favor a more harm-based and sector-specific breach notification framework. As previously stated, under the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, covered entities must notify the NYDFS within 72 hours of determining that a cybersecurity event has occurred, particularly if it is reasonably likely to cause material harm.[8] Similarly, under the FTC's 2023 Health Breach Notification Rule amendments, applicable to health-related FinTechs, non-HIPAA-covered entities must report qualifying breaches within 60 days if consumer health information is involved.9

1 Ministry of Electronics and Information Technology, Directions Under Section 70B of the IT Act, 2000, April 28, 2022.
2 Id. para 4(a).
3 Id. Annexure I.
4 Id. para 4(g).
5 Id. para 4(f).
6 Id. para 5(a).
7 Internet Society, Internet Impact Brief: India – CERT-In Cybersecurity Directions 2022, at 3–5 (June 1, 2022).
8 23 N.Y.C.R.R. § 500.17(a) (NYDFS Cybersecurity Regulation).
9 16 C.F.R. § 318.3 (FTC Health Breach Notification Rule).

Moreover, even in the financial sector more broadly, breach notification standards arise from the Interagency Guidance on Response Programs under the Gramm-Leach-Bliley Act (GLBA), issued by the Federal Reserve, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC). This guidance requires prompt notice to customers when there is unauthorized access to sensitive customer information but does not impose a statutory notification window, unlike in India.[10]

As such, American standards seem to reflect a more discretionary and outcomes-focused approach, in contrast with India's rules-based and precautionary ethos, where even potential or attempted attacks may trigger disclosure obligations.[11] What this means for fintech firms accustomed to U.S. thresholds is they may often struggle to reconcile Indian requirements with their existing global incident response playbooks. Delays in reporting or improper classifications of events can lead to non-compliance, reputational damage, and penalties under India's IT Act or anticipated enforcement from the Data Protection Board under the DPDPA once operational.[12]

For example, the CERT-In Directions were cited as a key compliance hurdle in a NASSCOM and DSCI paper, as they create compliance uncertainty and impede industry adoption and confidence.[13] This lack of harmonization between Indian and international standards can act as a barrier to investment and cross-border data flows as companies that process data in India via third-party vendors or shared cloud infrastructure must ensure that their detection and escalation protocols are both jurisdiction-aware and fully localized.[14]

In addition to CERT-In's mandates, India's financial regulators also have embedded incident reporting requirements into sector-specific frameworks. The Reserve Bank of India (RBI), for example, requires banks and payment operators to maintain 24/7 incident response teams and to report breaches within specified timelines under its Master Direction on Digital Payment Security Controls.[15] Similarly, the Insurance Regulatory and Development Authority of India (IRDAI) mandates periodic cyber audits and prompt disclosure of significant security incidents in its Guidelines on Information and Cyber Security for Insurers.[16]

Taken together, this overlapping regulatory structure significantly heightens the compliance risk landscape for fintech firms operating in India. A firm subject to RBI, IRDAI, and CERT-In oversight may face a sort of triple-reporting obligation for a single cyber incident, each with different timelines, formats, and disclosure thresholds. Further complexity arises when the incident involves cross-border data flows, as disclosures to foreign regulators (e.g., the SEC, FTC, or NYDFS) may trigger data sovereignty or supervisory access concerns under Indian law.

In response to these conditions, fintech firms are increasingly adopting a data localization-aware incident response playbooks, maintaining redundant logging infrastructure in India, automating compliance workflows, and entering into contractual arrangements with cloud providers and third-party vendors that ensure CERT-In alignment. Moreover, some U.S.-based firms have also begun to maintain India-specific Security Operations Centers (SOCs) and real-time monitoring tools to meet localized detection requirements.[17] Nonetheless, in the long term, unless harmonized breach reporting standards or mutual recognition frameworks

10 Office of the Comptroller of the Currency (OCC), Bulletin 2005-13, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, March 29, 2005.

11 Baker McKenzie, Global Data & Cybersecurity Handbook: India, December 20, 2024.

12 DLA Piper, Data Protection Laws of the World: India, updated January 6, 2025.

13 NASSCOM & DSCI, Representation to CERT-In on the Cybersecurity Directions, 2022, October 7, 2022.

14 CUTS International, Data Localisation: India's Double-Edged Sword, 2019.

15 Reserve Bank of India, Master Direction on Digital Payment Security Controls, DPSS.CO.OSD No.3941/06.08.005/2020-21, February 18, 2021.

16 Insurance Regulatory and Development Authority of India (IRDAI), Guidelines on Information and Cyber Security for Insurers, September 2017.

17 Aniket Bhosle, The Digital Payments Ecosystem of India: Planning Security Today for a Resilient Tomorrow, EY India, April 2, 2025.

emerge, the cost of compliance in India will remain disproportionately high for foreign firms. As such, for now, American fintech firms evaluating cross-border market entry into India clearly must treat cybersecurity not just as a technical function but as a jurisdictionally dynamic legal compliance obligation, with potential civil and criminal liability implications.

Tokenization, Payment Architecture, and Market Entry Strategy

Fintech firms looking to do business in India must understand how India's tokenization and payment architecture regulations represent one of the clearest fault lines between Indian and U.S. data governance regimes in the BFSI sector. While prior sections have discussed India's data localization mandates and cross-border transfer constraints (Sections 1.2–1.3), this section explores how India's evolving payment framework, particularly RBI's tokenization and card-on-file (CoF) regulations, disrupt standard operating practices for fintech firms accustomed to U.S. norms. These restrictions are not merely technical; they also reflect India's broader strategic approach to financial data sovereignty and consumer protection and have critical implications for market entry and infrastructure planning.

To better understand the potential challenges facing U.S.-based fintech firms, consider the Reserve Bank of India's (RBI) 2021 Circular on Card-on-File Tokenization (CoFT), which prohibits merchants, payment aggregators, and intermediaries from storing card credentials after transactions. Instead, tokenization, the process of replacing sensitive card details with a unique, non-sensitive identifier, is mandated, with only card networks or RBI-authorized Token Requestors permitted to perform this function.[1] This effectively ends the practice of merchants retaining user card details for convenience or subscription billing. Moreover, a hard compliance deadline of January 1, 2022, was enforced, requiring all actors to purge previously stored card data or face regulatory consequences.[2] As detailed in prior RBI circulars and FAQs, this move aims to "enhance security and safeguard consumers against fraud," especially amid growing digital payments adoption in India.[3]

The RBI's tokenization policy also builds upon earlier frameworks, particularly the 2020 Guidelines on Regulation of Payment Aggregators and Payment Gateways.[4] These guidelines restrict data storage practices, require merchant registration, and establish baseline compliance obligations for aggregators, such as maintaining escrow accounts, cybersecurity protocols, and periodic audits. Most importantly, they prohibit the storage of cardholder data except for truncated card numbers and issuer names, dovetailing with the CoFT policy. For U.S.-based fintech firms that rely on card-on-file architecture, token reuse, and integrated billing solutions, this means a complete overhaul of their backend systems, and thus presents significant complications.

In contrast, the U.S. regulatory framework—largely shaped by the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and the Federal Trade Commission (FTC) Safeguards Rule, does not prescribe a tokenization regime. U.S. firms may retain card data if they implement "reasonable administrative, technical, and physical safeguards."[5] While many PCI-DSS standards are followed in practice and tokenization is encouraged as a risk mitigation tool, it remains voluntary unless imposed through contractual terms or state-level consent regimes. Even under more stringent laws like California's Consumer Privacy Rights Act (CPRA), there is no legal requirement to tokenize or delete financial data unless requested by consumers.[6]

1 Reserve Bank of India, Card-on-File Tokenisation (CoFT) Circular, DPSS.CO.PD No.1463/02.14.003/2021-22 (Sept. 7, 2021).

2 Reserve Bank of India, FAQs on Tokenisation, (Dec. 2021)

3 Ibid.

4 Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, DPSS.CO.PD.No.1810/02.14.008/2019-20 (Mar. 17, 2020).

5 Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2024).

6 Cal. Civ. Code § 1798.105 (West 2023) (California Consumer Privacy Rights Act).

This showcases a clear divergence in regulatory philosophy, with India's ex-ante prohibition and mandate versus the U.S.'s ex-post accountability model, which can quickly translate into friction for fintech firms. For instance, recurring billing models widely used by U.S. platforms like Stripe, Square, and Plaid depend on storing and reusing card data, which becomes unviable under India's CoFT regime. Moreover, these firms often operate on global architecture that routes and stores payment data across multiple jurisdictions, creating incompatibility with RBI's "India-only" storage rules discussed in Section 1.2.

As seen in prior sections, these differences have already caused problems. In 2021, the RBI barred Mastercard from onboarding new customers due to non-compliance with localization and tokenization norms, even after years of operating in India.[7] Though the ban was eventually lifted, this underscored the RBI's assertiveness and unwillingness to accommodate legacy practices or global brand exceptions. Other global firms, including Visa and American Express, were similarly placed under scrutiny. This forced them to accelerate efforts to comply with RBI-prescribed infrastructure models. For newer entrants or smaller fintech players lacking the resources to negotiate or co-develop tokenization platforms with Indian partners, these requirements may raise the threshold for market entry altogether.[8]

Thus, from a compliance planning perspective, it is imperative that U.S. fintech firms entering India incorporate several steps. First, they must integrate with licensed token requestors, typically Indian banks or card networks like NPCI, Visa, or Mastercard India. Second, they should design systems that handle token provisioning, lifecycle management, and user mapping, while ensuring tokens are not reused across merchants, in line with RBI guidance. Third, they must re-architect billing systems to accommodate non-persistent card data and meet audit readiness standards imposed by the RBI.

India's tokenization framework introduces substantial legal and operational burdens for foreign fintech firms. These include capital expenditure, legal vetting, and changes to user flows, for example, requiring re-authentication for recurring payments. While UPI offers an alternative, its architecture differs markedly from card networks used in the U.S., forcing companies to adjust both backend compliance and frontend interfaces. The legal implications go beyond cost: tokenized credentials and logs must be stored locally, subject to audit and six-hour breach notification under the CERT-In Directions (Apr. 28, 2022). Firms must synchronize to NIC/NPL-certified time servers and retain logs for 180 days. In contrast, U.S. standards such as NYDFS 23 N.Y.C.R.R. Part 500 and FTC rules allow longer timelines and more internal discretion—heightening compliance friction in the event of breaches involving tokenized data.[9]

Ultimately, tokenization and payment data architecture remain one of the most challenging friction points in cross-border fintech expansion. U.S.-based firms should treat India's regulatory architecture not as a minor variation but as a structurally different model, with high stakes for failure. A proactive partnership with Indian legal counsel, early technical integration with licensed entities, and executive-level engagement with the RBI would be critical to support sustainable market entry into the Indian fintech ecosystem.

7 Reserve Bank of India, Press Release: Restrictions on Mastercard Asia/Pacific Pte. Ltd., PR No. 2021-2022/710 (July 14, 2021).

8 OECD, Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses (Dec. 2021).

9 N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2023); see also 16 C.F.R. § 314 (2024).

Regulatory Divergence and the Need for Interoperability

While India and the United States share deep commercial ties in the fintech sector, it is clear that their respective data protection regimes remain fundamentally divergent in structure, enforcement philosophy, and jurisdictional design. For fintech firms operating across both markets, this divergence creates legal uncertainty, increased compliance costs, and risks of inadvertent regulatory breaches. For while India's approach is characterized by centralized authority under the Digital Personal Data Protection Act, 2023 (DPDPA), and reinforced through sectoral mandates from the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), and Indian Computer Emergency Response Team (CERT-In). This stands in in stark contrast to the decentralized, sectoral, and state-driven model of the U.S., which is anchored in laws such as the Gramm-Leach-Bliley Act (GLBA), state privacy laws like the California Consumer Privacy Act (CCPA), and overlapping agency rules from the Federal Trade Commission (FTC) and New York Department of Financial Services (NYDFS).[1]

As discussed in prior sections, India's DPDPA provides a horizontal framework applicable to all personal data processing activities, including extraterritorial operations by foreign entities that offer goods or services to individuals in India. It establishes a consent-centric model, limits cross-border data transfers through a government-controlled negative list, and can impose significant penalties for noncompliance, up to ₹250 crore (approximately USD $30 million) per violation.[2] U.S. law, on the other hand, lacks a singular national privacy law. Thus, the GLBA governs financial institutions, and while it does emphasize notice, opt-out provisions, and the Safeguards Rule, it does not impose any localization or extraterritorial compliance requirements.[3] These differences mean that a U.S.-based fintech firm entering the Indian market must implement a substantially more restrictive and proactive privacy regime than it might apply domestically.[4]

As such, these divergences can significantly increase compliance friction, particularly in cross-border transfers. For instance, India may prohibit transfers to jurisdictions lacking adequate protections or reciprocal obligations, while the U.S. maintains no formal outbound restriction on financial data flows. As such, bilateral transfers could become asymmetrical: permissible under U.S. law but barred by Indian regulation. This creates structural uncertainty for firms handling Indian customer data using U.S.-based cloud providers or global payment networks. Moreover, while Draft DPDPA rules circulated in early 2025 indicated that India may evaluate destination countries based on enforcement capacity, reciprocity, and misuse prevention, a criterion unlikely to be uniformly met by U.S. state or sectoral privacy regimes.[5]

Thus, the absence of a common regulatory bridge increases the burden on compliance teams. Fintech firms must conduct jurisdiction-specific impact assessments, develop data transfer risk mitigation strategies such as Standard Contractual Clauses or Binding Corporate Rules, for example, and allocate additional legal resources to monitor evolving transfer restrictions. These are especially burdensome for mid-sized players lacking in-house legal capacity. Thus, in this context, interoperability emerges as a pragmatic objective.

1 Digital Personal Data Protection Act, 2023, §§ 2, 4, 5, 33 (India); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2024); California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (West 2023); 23 N.Y. Comp. Codes R. & Regs. § 500 (2023); Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2024).

2 Digital Personal Data Protection Act, 2023, §§ 7, 16, 33 (India).

3 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2024).

4 Digital Personal Data Protection Act, 2023, §§ 5–16 (India).

5 Nishith Desai Associates, Fintech Compendium (2025).

It would be advisable for regulatory bodies in both countries to support frameworks that allow mutual recognition of data safeguards based on shared principles such as purpose limitation, data minimization, and accountability. This could take the form of a bilateral agreement or a memorandum of understanding modelled loosely on the EU–U.S. Data Privacy Framework.[6] It could also draw from global protocols that already enable secure data exchange in sensitive domains, such as ISO 20022 for cross-border payments and SWIFT messaging standards, which function despite underlying legal disparities by embedding technical and governance assurances.[7] Ultimately, while some regulatory divergence is likely to persist, legal interoperability can mitigate its operational consequences. For fintech firms navigating India and the U.S., structured dialogue between regulators and alignment on transfer safeguards can reduce compliance overhead and offer greater legal predictability across jurisdictions.

Case for a U.S.–India Data Transfer Framework through Mutual Recognition or Interoperability Across Data Regimes

As cross-border fintech operations intensify it is in the interest of firms across India and the United States to establish a robust, legally grounded, and industry-sensitive data transfer framework. As despite the regulatory divergence between India's Digital Personal Data Protection Act, 2023 (**"DPDPA"**) and the United States' sectoral, state-driven data protection regime, there exists a compelling legal and commercial rationale for bilateral regulatory interoperability, particularly in the BFSI domain.

As the situation currently stands India's DPDPA permits cross-border data transfers unless the Central Government restricts specific jurisdictions or classes of data under Section 16.[8] The Ministry of Electronics and Information Technology (MeitY) has floated draft rules identifying factors such as reciprocal legal protections, enforcement capacity, and commitments to prevent misuse as criteria for determining "trusted" destinations.[9] This architecture, based on government-led negative listing, does differ fundamentally from the United States' permissive approach, which lacks national restrictions on outbound data transfers. Instead, the U.S. legal model relies on private ordering through contractual clauses, regulatory guidance (e.g., from the FTC), and sector-specific obligations such as those under the Gramm-Leach-Bliley Act and Safeguards Rule.[10]

This asymmetry in legal assumptions, India's emphasis on government authorization versus the U.S.'s reliance on risk-based self-regulation, clearly creates friction for fintech firms seeking legal certainty and operational efficiency. For example, a U.S.-based payment gateway or neobank expanding into India must comply with the RBI's data localization directives and limit offshore processing, while the DPDPA could further restrict which jurisdictions are eligible for data transfer. Conversely, Indian FinTechs exporting data to the U.S. may find themselves grappling with California Consumer Privacy Act (CCPA) provisions for cross-contextual behavioral advertising, breach notification rules under New York's SHIELD Act, and regulatory exposure under Section 5 of the Federal Trade Commission Act.[11]

---

6 U.S. Department of Commerce, EU-U.S. Data Privacy Framework, available at: https://www.dataprivacyframework.gov.

7 International Organization for Standardization, ISO 20022 Financial Services — Universal Financial Industry Message Scheme, ISO 20022:2013 (4th ed. 2013); Society for Worldwide Interbank Financial Telecommunication (SWIFT), SWIFT Messaging.

8 Digital Personal Data Protection Act, 2023, § 16 (India).

9 Nishith Desai Associates, Fintech Compendium (2025)

10 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2024); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2024).

11 California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (West 2023); New York Stop Hacks and Improve Electronic Data Security Act, N.Y. Gen. Bus. Law § 899-bb (McKinney 2023); Federal Trade Commission Act, 15 U.S.C. § 45 (2024).

Against this backdrop, however, it is clear how a bilateral U.S.–India data transfer framework modelled on mutual recognition or interoperability could mitigate uncertainty while preserving each country's constitutional and regulatory autonomy. This framework could resemble the now-defunct EU–U.S. Privacy Shield or the current Data Privacy Framework (DPF), but adapted for sector-specific realities.[12]

Core pillars might include:

- Reciprocal adequacy findings for limited categories of BFSI data, grounded in enforceable protections and dispute resolution mechanisms;
- Binding corporate rules (BCRs) or standardized contractual clauses recognized across both jurisdictions;
- Institutional cooperation between the U.S. Department of the Treasury, Federal Trade Commission (FTC), and Indian regulators like the Data Protection Board of India, the Reserve Bank of India (RBI), and the Insurance Regulatory and Development Authority of India (IRDAI).
- Designated redress mechanisms, potentially modelled on arbitration or ombudsman systems.

Such a framework would not require full harmonization of privacy laws. Rather, it would reflect a shared commitment to foundational principles such as lawfulness, fairness, security, purpose limitation, and accountability, while enabling commercial data flows essential to digital finance. It could also evolve into a multi-phase structure: beginning with financial data, expanding to cloud services, and eventually influencing broader trade negotiations in digital services.

So far, India and the U.S. have both signalled interest in deepening digital cooperation through the U.S.–India Commercial Dialogue, the U.S.–India Strategic Trade Dialogue, and joint G20 initiatives on digital public infrastructure. 13 As India's DPI model gains international recognition and the U.S. continues to advance sectoral regulation through agencies like the FTC and NYDFS, the legal and diplomatic scaffolding for a data transfer accord already exists. Ultimately, Fintech firms, especially those seeking first-mover advantage, stand to benefit from engaging proactively with regulators and industry associations to help shape such a framework. Through proactive alignment with emerging interoperability principles, firms can avoid fragmented legal exposure, streamline operations, and build reputational capital in both jurisdictions.

Leveraging Global Financial Data Standards to Support Cross-Border Interoperability

Bilateral frameworks between India and the U.S. offer one strategic path for resolving regulatory friction. However, Fintech firms should also take note of existing global financial data protocols that provide a tested blueprint for operational interoperability. These protocols, although originally designed for transaction integrity, financial messaging, or anti-money laundering (AML) purposes, can serve as precedents for creating a shared compliance language across borders. Particularly for U.S.-based FinTechs seeking entry into or expansion within the Indian market, aligning with these standards can ease regulatory navigation and demonstrate institutional maturity.

12 U.S. Department of Commerce, EU–U.S. Privacy Shield Framework (archived); U.S. Department of Commerce, EU–U.S. Data Privacy Framework, available at : https://www.dataprivacyframework.gov.

13 U.S.–India Commercial Dialogue, India–U.S. Bilateral Relations Brief (Jan. 27, 2025),

A prime example is the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, which provides a global messaging system for financial transactions. SWIFT's message standards (such as MT and the more recent ISO 20022 XML schemas) enable interoperability between thousands of financial institutions worldwide.[14] Although SWIFT itself does not handle funds or enforce privacy rules, its structured messaging formats have been universally adopted and are already recognized by Indian and American banks and regulators. ISO 20022, in particular, has been endorsed by the Reserve Bank of India (RBI) for real-time gross settlement systems and by U.S. institutions such as the Federal Reserve for Fedwire migration.[15] For FinTechs designing payment systems or core banking platforms, compliance with ISO 20022 can be an asset in aligning with both countries' evolving infrastructure requirements.

Moreover, the Financial Action Task Force (FATF) Recommendations, especially Recommendation 15 on new technologies and Recommendation [16] on wire transfers, provide a harmonized set of compliance obligations for AML and Countering the Financing of Terrorism (CFT) programs. 16 These standards are integrated into India's Prevention of Money Laundering Act, 2002 (PMLA) and the Know Your Customer (KYC) Master Direction from the RBI, as well as in U.S. law through the Bank Secrecy Act (31 U.S.C. §§ 5311–5330) and FinCEN's rules.[17] By designing products that are FATF-compliant from the outset, fintech firms can avoid duplicative risk management architecture and demonstrate their preparedness to regulators across jurisdictions.

Furthermore, the Basel Committee on Banking Supervision's standard BCBS 239, "Principles for effective risk data aggregation and risk reporting", sets global expectations for data governance in systemically important financial institutions.[18] While not binding per se, BCBS 239 has influenced RBI's supervisory expectations and is broadly referenced in the U.S. by prudential regulators like the Federal Reserve and the Office of the Comptroller of the Currency (OCC).[19] Compliance with BCBS 239 or related best practices like those issued by the International Organization of Securities Commissions (IOSCO) for fintech and crypto-assets can show a proactive commitment to regulatory discipline and resilience.

On the privacy front, India's alignment with the OECD Privacy Guideline, particularly regarding accountability, data minimization, and transborder flow, offers another layer of interoperability.[20] The United States, while not adopting omnibus privacy law, has endorsed OECD principles in various multilateral negotiations and continues to engage with the APEC Cross-Border Privacy Rules (CBPR) framework.[21] These frameworks emphasize mutual recognition and accountability-based cross-border data governance, principles that FinTechs can internalize through privacy-by-design, data audit mechanisms, and certification programs.

14 Int'l Org. for Standardization, ISO 20022 Financial Services — Universal Financial Industry Message Scheme, ISO 20022:2013 (4th ed. 2013).

15 Reserve Bank of India, Access for Non-Banks to Centralised Payment Systems – FAQs (July 28, 2021).

16 Fin. Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations (updated Mar. 2022),

17 Prevention of Money Laundering Act, No. 15 of 2003, § 12, India Code (2003), and Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016, RBI/DBR/2015-16/18 (as updated July 2023).

18 Basel Comm. on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239), Bank for Int'l Settlements (Jan. 2013).

19 Reserve Bank of India, Guidelines on Data Governance in Banks ¶ 2.1 (Apr. 2021) and Bd. of Governors of the Fed. Reserve Sys. & Off. of the Comptroller of the Currency, Joint Statement on Risk Management for Cloud Computing Services (Apr. 30, 2020),

20 Org. for Econ. Co-operation & Dev. (OECD), The OECD Privacy Framework (2013), and Ministry of Electronics & Info. Tech., White Paper on a Data Protection Framework for India 17–20 (2017),

21 U.S. Dep't of Com., Privacy Shield Framework: U.S. Commitment to the OECD Privacy Principles, and Asia-Pacific Econ. Coop. (APEC), Cross-Border Privacy Rules (CBPR) System,

Thus, it is clear that fintech firms that anchor their compliance architecture in these global standards position themselves to adapt to both bilateral and multilateral developments in data governance. Through demonstrating adherence to well-established global protocols, firms can potentially benefit from "presumptive adequacy" in regulatory assessments. They may be able to ease onboarding processes with banks and insurers, and reduce the friction of legal review in both jurisdictions. This approach also signals institutional credibility to investors, regulators, and consumers alike. Over time, these efforts may also help lay the foundation for a more formal global interoperability framework, possibly modelled on sector-specific regimes like the APEC CBPR system or technical protocols such as ISO 20022 and SWIFT.

Conclusion

This paper has provided a comparative legal and regulatory analysis of the data protection regimes governing the Banking, Financial Services, and Insurance (BFSI) sectors in India and the United States, with a focus on cross-border fintech operations. As digital finance becomes increasingly globalized, regulatory divergence between jurisdictions has emerged as a critical operational concern. India and the United States represent two contrasting models: one centralized and vertically layered, the other federated and sectoral. Understanding these models is essential for fintech firms seeking to design compliant systems, manage risk, and structure sustainable market entry strategies.

In India, the recently enacted Digital Personal Data Protection Act, 2023 (DPDPA) establishes a consent-driven, rights-based framework that cuts across sectors. However, the BFSI domain is additionally governed by a dense mesh of sectoral mandates and faces a stacked enforcement model. The Reserve Bank of India (RBI) requires that all payment system data be stored exclusively in India, with limited exceptions.[1] The Insurance Regulatory and Development Authority of India (IRDAI) mandates that insurers store policyholder data on servers located within the country.[2] Meanwhile, the Indian Computer Emergency Response Team (CERT-In) imposes aggressive breach notification and log retention requirements, including six-hour incident reporting and synchronization of system clocks with Indian Standard Time.[3] These obligations do not merely coexist with DPDPA; they intensify its compliance impact by adding regulator-specific penalties, timelines, and operational standards.

In contrast, the United States follows a fragmented but flexible regime. The Gramm-Leach-Bliley Act (GLBA) forms the federal backbone for privacy and security in financial institutions, with its Privacy, Safeguards, and Pretexting Rules.[4] However, enforcement is distributed across a network of actors, including the Federal Trade Commission (FTC), Office of the Comptroller of the Currency (OCC), Federal Reserve, FDIC, and state regulators such as the New York Department of Financial Services (NYDFS).[5] Unlike India, the U.S. permits outbound data transfers without geographical restrictions, relying instead on contractual mechanisms and risk assessments. However, complexity arises from a growing number of state-level privacy statutes, such as the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), and similar laws in Colorado, Connecticut, and Utah.[6]

These differences also carry many practical implications for cross-border fintech firms. Indian regulation imposes non-derogable compliance costs. Firms must often establish localized infrastructure, ensure segregated data environments, and build incident response systems that adhere to multiple overlapping mandates. U.S. firms expanding into India thus face challenges do not present in their home jurisdiction, where flexibility and private ordering through contractual clauses is the norm. Moreover These divergences lead to three categories of operational strain: (1) compliance infrastructure duplication, especially around tokenization, encryption, and cloud architecture; (2) breach response dissonance, where firms must tailor incident management plans to multiple jurisdictions' reporting deadlines and escalation standards; and (3) legal review friction, as firms must localize privacy notices, vendor agreements, and data processing addenda

1 RBI, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-18 (Apr. 6, 2018).

2 IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3.

3 CERT-In, Directions under Section 70B, IT Act, 2000 (Apr. 28, 2022).

4 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018).

5 23 N.Y.C.R.R. Part 500 (2023).

6 Cal. Civ. Code §§ 1798.100–1798.199 (2023); Va. Code Ann. § 59.1–581.5(A)(1) (2023).

to meet the higher of either Indian or U.S. standards. Moreover since the process of the implementation of (DPDP) Rules India has operationalised its data-protection architecture through final rules and formal institutional establishment, whereas the United States has continued to deepen its patchwork through state privacy expansion, cybersecurity enforcement, and new but not yet fully settled consumer-financial-data rulemaking.[7]

The burden is particularly acute in the BFSI domain due to the sensitive nature of financial data and the high degree of regulatory oversight. Firms operating in both jurisdictions must often create segmented compliance teams and legal architectures that track parallel regimes. Moreover, cross-border coordination becomes riskier when enforcement environments are unpredictable or where disclosure to one authority (e.g., CERT-In) could trigger scrutiny or liability in another.

In light of these challenges, this paper recommends that cross-border fintech firms adopt a harmonization-by-design strategy. This includes anchoring compliance architecture to internationally recognized frameworks such as the OECD Privacy Guidelines,[8] the APEC Cross-Border Privacy Rules (CBPR),[9] the Financial Action Task Force (FATF) digital ID standards,[10] and the Basel Committee's BCBS 239 risk data principles.[11] Firms that demonstrate adherence to these global protocols may benefit from "presumptive adequacy" in regulatory audits, smoother onboarding processes with regulated entities, and reduced legal review friction. Moreover, such alignment signals institutional credibility to investors, regulators, and consumers.

The paper further argues that regulators in both India and the United States should explore bilateral interoperability frameworks, especially in the BFSI sector. A model agreement on cross-border data transfers, akin to a fintech-specific "safe harbour", could significantly reduce redundancy and provide legal clarity. While such cooperation is politically and technically complex, precedents exist in financial governance. Protocols such as SWIFT, ISO 20022, and BCBS 239 demonstrate that multilateral data infrastructure can coexist with national sovereignty when aligned with global risk, accountability, and security principles.[12]

In conclusion, the regulatory divergence between India and the United States presents both challenges and opportunities for fintech firms. Compliance with these norms is thus a strategic necessity that shapes a firm's ability to scale, secure investment, and sustain long-term cross-border operations. As such, navigating the complexity of dual regimes requires more than reactive compliance; it demands proactive legal design, strategic harmonization, and a forward-looking regulatory dialogue. As financial data becomes increasingly critical to economic infrastructure and individual rights, developing a shared framework for interoperability in the BFSI sector should be the ideal.

7 Digital Personal Data Protection Rules, 2025; Ministry of Electronics and Information Technology Notification establishing the Data Protection Board of India, 13 Nov. 2025; National Conference of State Legislatures, Summary 2024 Consumer Data Privacy Legislation; Consumer Financial Protection Bureau, Personal Financial Data Rights (updated Jan. 2026).

8 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

9 APEC, Cross-Border Privacy Rules System (2015).

10 FATF, Guidance on Digital Identity (2020).

11 Basel Committee on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239) (2013).

12 Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Sources/Additional Reading

1. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Extraordinary, Part II, sec. 1 (Aug. 11, 2023).
   https://egazette.nic.in/WriteReadData/2023/248945.pdf
2. Reserve Bank of India, Storage of Payment System Data, Circular No. DPSS.CO.OD No.2785/06.08.005/2017-2018 (Apr. 6, 2018).
   https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI166B0BD8053D9D24B8281537E466891F9A4.PDF
3. Insurance Regulatory and Development Authority of India (IRDAI), Maintenance of Insurance Records Regulations, Reg. 3, Gazette of India, No. IRDA/Reg/20/107/2015 (July 31, 2015).
   https://irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo2623&flag=1
4. Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022).
   https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
5. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (2018).
   https://www.govinfo.gov/content/pkg/USCODE-2018-title15/html/USCODE-2018-title15-chap94-subchapI-sec6801.htm
6. New York Department of Financial Services (NYDFS), Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500 (2023).
   https://govt.westlaw.com/nycrr/Document/I9f6d3f9e05fe11e78b918b83fa49a135
7. California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100–1798.199 (as amended by CPRA).
   https://oag.ca.gov/privacy/ccpa
8. Virginia Consumer Data Protection Act (VCDPA), Va. Code Ann. § 59.1–581.5(A)(1) (2023).
   https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-581.5/
9. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).
   https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
10. APEC, Cross-Border Privacy Rules (CBPR) System (2015).
    https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy/CBPR
11. Financial Action Task Force (FATF), Guidance on Digital Identity (March 2020).
    https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-on-Digital-Identity.html
12. Basel Committee on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239), Bank for International Settlements (Jan. 2013).
    https://www.bis.org/publ/bcbs239.htm
13. International Organization for Standardization, ISO 20022: Universal Financial Industry Message Scheme, ISO TC 68/SC 9.
    https://www.iso20022.org
14. SWIFT (Society for Worldwide Interbank Financial Telecommunication), About SWIFT.
    https://www.swift.com
15. NASSCOM–DSCI, India's Trillion Dollar Digital Opportunity: A Roadmap for Fintech, Healthtech and Agritech (2023).
    https://www.dsci.in/content/indias-trillion-dollar-digital-opportunity

16. Nishith Desai Associates, India's Flourishing Fintech Flambeau: Regulation & Innovation in the Digital Age (2025).
https://www.nishithdesai.com

17. Vidhi Centre for Legal Policy, Cross-Border Data Transfers: Assessing India's Legal and Policy Framework (2022).
https://vidhilegalpolicy.in/research/cross-border-data-transfers/

18. Observer Research Foundation (ORF), Trisha Ray et al., Trusted Data Flows: Aligning India's Data Transfer Rules with Global Standards, ORF Occasional Paper No. 359 (2022).
https://www.orfonline.org/research/trusted-data-flows/

19. Carnegie India, Arindrajit Basu & Elonnai Hickok, The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India (2019).
https://carnegieindia.org/2019/06/27/localisation-gambit-pub-79408

20. BSA | The Software Alliance, Data Protection and Digital Transformation in India: Recommendations for a Forward-Looking Framework (2023).
https://www.bsa.org/policy-filings/india-data-protection

21. Internet and Mobile Association of India (IAMAI), Position Paper on Data Privacy and Cross-Border Data Flow (2022).
https://www.iamai.in/

22. Brookings Institution, Joshua P. Meltzer, The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment (2014).
https://www.brookings.edu/research/the-importance-of-the-internet-and-transatlantic-data-flows-for-u-s-and-eu-trade-and-investment/

23. Atlantic Council, Justin Sherman, Data Diplomacy: Digital Sovereignty and the Global Battle for Data Flows (2021).
https://www.atlanticcouncil.org/in-depth-research-reports/report/data-diplomacy/

24. Internet Society, Moving Toward a Data-Driven Economy: Enabling Data Flows to Realize the Benefits of the Internet (2021),
https://www.internetsociety.org/resources/doc/2021/enabling-data-flows/.

25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

26. Vidhi Centre for Legal Policy, Comments on the Draft Digital Personal Data Protection Bill, 2022 (Jan. 2023),
https://vidhilegalpolicy.in/research/comments-on-the-digital-personal-data-protection-bill-2022/.

27. Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Sess. (Utah 2022), codified at Utah Code Ann. §§ 13-61-101 to 13-61-502.

28. Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, Notification S.O. 5082(E), Gazette of India, Extraordinary, Part II, sec. 3(i) (Nov. 13, 2025),
https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf.

29. Ministry of Electronics and Information Technology, Notification establishing the Data Protection Board of India, Gazette of India, Extraordinary, Part II, sec. 3(ii) (Nov. 13, 2025),
https://www.meity.gov.in/static/uploads/2025/11/cc217843dc3bcb37b2b05bcc3b4e031f.pdf.

30. Ministry of Electronics and Information Technology, Notification specifying the number of members of the Data Protection Board of India, Gazette of India, Extraordinary, Part II, sec. 3(ii) (Nov. 13, 2025),
https://www.meity.gov.in/static/uploads/2025/11/f6c0837972422cf79d890bfe84cc04d6.pdf.

31. Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security (Sept. 2, 2022), https://irdai.gov.in/document-detail?documentId=1354286.

32. Insurance Regulatory and Development Authority of India, Circular on Cyber Incident or Crisis Preparedness, Ref. No. IRDAI/GA&HR/CIR/MISC/49/03/2025 (Mar. 24, 2025), https://irdai.gov.in/documents/37343/365525/%E0%A4%B8%E0%A4%BE%E0%A4%87%E0%A4%AC%E0%A4%B0%2B%E0%A4%98%E0%A4%9F%E0%A4%A8%E0%A4%BE%2B%E0%A4%AF%E0%A4%BE%2B%E0%A4%B8%E0%A4%82%E0%A4%95%E0%A4%9F%2B%E0%A4%95%E0%A5%80%2B%E0%A4%A4%E0%A4%A4%E0%A5%8D%E0%A4%AA%E0%A4%B0%E0%A4%A4%E0%A4%BE%2B%E0%A4%AA%E0%A4%B0%2B%E0%A4%AA%E0%A4%B0%E0%A4%BF%E0%A4%AA%E0%A4%A4%E0%A5%8D%E0%A4%B0%2B_%2BCircular%2Bon%2BCyber%2BIncident%2Bor%2BCrisis%2BPreparedness.pdf/2b53047f-cf15-ea35-f8af-882a3150ef2c?download=true&t=1742966637149&version=1.0.

33. Federal Trade Commission, Safeguards Rule Notification Requirement Now in Effect (May 14, 2024), https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect.

34. Consumer Financial Protection Bureau, Personal Financial Data Rights, https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/personal-financial-data-rights/.

35. National Conference of State Legislatures, Summary 2023 Consumer Data Privacy Legislation (Sept. 28, 2023), https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation.

36. National Conference of State Legislatures, 2024 Consumer Data Privacy Legislation, https://www.ncsl.org/technology-and-communication/2024-consumer-data-privacy-legislation.

37. New York Department of Financial Services, Cybersecurity: Part 500 Requirement Checklist for DFS-Regulated Entities with § 500.19(a) Limited Exemptions, https://www.dfs.ny.gov/industry_guidance/cybersecurity/pt500_require_checklist_regulated_entities_limited_exemptions.

38. New York Department of Financial Services, Superintendent Harris Secures More than $19 Million from Auto Insurance Companies over Data Breaches (Oct. 14, 2025), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20251014.

39. National Association of Insurance Commissioners, Materials - Innovation, Cybersecurity, and Technology (H) Committee (Mar. 25–26, 2026), https://content.naic.org/sites/default/files/national_meeting/Materials-H-Cmte032526_0.pdf.

40. Colorado Privacy Act, S.B. 21-190, 73rd Gen. Assemb., 1st Reg. Sess. (Colo. 2021), codified at Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313.

41. Ministry of Electronics & Info. Tech., Cross-Border Data Flow: Note on Trusted Geographies, Digital India Dialogue Series (2024), https://www.meity.gov.in.

42. Reserve Bank of India – NBFC Cybersecurity

43. Reserve Bank of India, Master Direction – Information Technology Framework for the NBFC Sector, DNBR. PD.CC.No. 090/03.10.001/2017-18 (June 8, 2017), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MDIT070620176F6BB19BFCE04C3585E3FDF10554C5F5.PDF.

44. IRDAI – 2023 Cybersecurity Guidelines

45. Insurance Regulatory & Dev. Auth. of India (IRDAI), Guidelines on Information and Cyber Security, Ref. No. IRDAI/IT/GDL/MISC/080/04/2023 (Apr. 24, 2023), https://irdai.gov.in.

46. CERT-In – FAQ Clarification on Directions

47. Indian Computer Emergency Response Team (CERT-In), FAQs on Directions Under Sub-Section (6) of Section 70B of the IT Act, 2000 (May 18, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_FAQ_18.05.2022.pdf.

48. European Data Protection Board (EDPB) – Supplementary Measures

49. European Data Protection Board (EDPB), Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0 (updated June 18, 2021), https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

50. U.S. Federal Trade Commission (FTC) – Breach Notification

51. Fed. Trade Comm'n, Data Breach Response: A Guide for Business (2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

52. CJEU Schrems II Decision Case C-311/18, Data Prot. Comm'r v. Facebook Ireland & Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311.

53. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India), https://indiankanoon.org/doc/91938676/.

54. TransUnion LLC v. Ramirez, 594 U.S. ___ (2021), https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

55. Puttsway v. Pennsylvania Dep't of Labor & Indus., 818 A.2d 598 (Pa. Commw. Ct. 2003).

56. Payment and Settlement Systems Act, No. 51 of 2007, § 18, Gazette of India, Extraordinary, Part II, sec. 1.

57. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Extraordinary, Part II, sec. 3(i).

58. International Monetary Fund (IMF), "Cybersecurity Risk Supervision: Practices and Recommendations," Monetary and Capital Markets Department, IMF Staff Discussion Note (June 2022).

59. International Organization for Standardization, ISO/IEC 27001: Information Security Management Systems — Requirements, ISO/IEC Standard (2013).

60. T for Change, India's Data Protection Law—A Step Forward or a Case of Regulatory Capture?, IT for Change (Aug. 2023), https://itforchange.net/index.php/India-Data-Protection-Law-Analysis.

61. Aditya Kalra, India says firms must get govt nod to transfer user data abroad under new law, Reuters (Aug. 7, 2023), https://www.reuters.com/world/india/india-says-firms-must-get-govt-nod-transfer-user-data-abroad-under-new-law-2023-08-07/.

62. Nishith Desai Associates. India's Flourishing Fintech Flambeau. April 2025. https://www.nishithdesai.com/SectionCategory/33/Research-and-Articles/12/FinTech/10801/India's-Flourishing-Fintech-Flambeau.html

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm — and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international law firm with Indian offices in Mumbai, New Delhi, Bangalore and GIFT City and foreign offices in New York, Palo Alto (Silicon Valley) and Singapore. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly — the VISION — to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech and Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times–RSG award 4 times in a row, (2014-2017) as the Most Innovative Indian Law Firm.

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled '**Management by Trust in a Democratic Enterprise**,' published by John Wiley & Sons, USA.

Management by Trust in a Democratic Enterprise: A Law Firm Shapes Organizational Behavior to Create Competitive Advantage

NISHITH DESAI

The founder of Mumbai-based Nishith Desai Associates (NDA) built his law firm on a few powerful ideas: a trust-based, nonhierarchical, democratically managed organization that leverages research and knowledge to deliver premium-service, high value, and a unique employer proposition that shatters many negative law-firm stereotypes. The author discusses the rationale behind NDA's business model and its organization and talent framework, and tracks the firm's philosophical genesis, which includes ideas from Mahatma Gandhi on democracy and from Charles Handy on trust in virtual organizations. He examines the implications of Handy's Rules of Trust for HR policies and practices, and then he describes NDA's approaches for creating challenge, growth, and rewards in a nonhierarchical structure; building behavioral competencies; balancing control with freedom; and other management practices that empower employees to act in the best interests of the firm and its clients. © 2009 Wiley Periodicals, Inc.

Think of a profession that, by its very nature and craft, tends to ingrain such attitudes as low trust, skepticism, and dispersion, where the personal interest and goals of individualistic, ambitious, self-driven, ego-led professionals supersede any commitment to the organization's goals. Chances are that the legal profession will be at the top of your list. If not, just think of a lawyer—and the description fits effortlessly. (As a lawyer, I have no qualms making this statement.)

Now, add to that the long-held fundamentals of running a competitive law firm. Profitability is driven by leverage (number of people) and hourly rate realization, which effectively means profitability is increased by working people more hours or hiring more people. Thus, what you tend to find is a sweatshop of overworked professionals with no work-life balance, high attrition, burnout, and indifferent loyalty. That apart, hierarchy, leverage, seniority bias, formality, and conservatism largely dominate a law firm environment. And what's more, this tends to typify law firms anywhere in the world.

Consequently, dodging the traditional law-firm constraints to create a very different organizational model, employer proposition, and culture is a tall order. But in our experience, it is a tremendous opportunity for value creation. It drives us to think "out of the box" and establish afresh a compelling culture, organization, and people strategy that would ultimately attract and retain the talent that we wanted for a longer-term competitive advantage.

For the two decades since its establishment in 1989 in Mumbai, India, our firm, Nishith Desai Associates (NDA), has been conceptualizing, implementing, and refining our approach to and practice of managing a democratic, trust-led enterprise that delivers high-value, premium-positioned legal services. That our approach has made some headway is indicated by NDA's growth—about 100 members and additional offices in India (Bangalore), the United States (Palo Alto, California), and Singapore—and

Published online in Wiley InterScience (www.interscience.wiley.com)
DOI: 10.1002/jon.XXXX

Research@NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our NDA Labs dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research papers and disseminate them through our website. Our ThinkTank discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. Imaginarium AliGunjan is a platform for creative thinking; an apolitical ecosystem that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness — that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have on our research publications. Please feel free to contact us at **research@nishithdesai.com**.

Recent Research Papers

Extensive knowledge gained through our original research is a source of our expertise.

February 2026

AI & Deep Tech Investments Landscape

A report from India Deep Tech Alliance (IDTA)

January 2026

Research Paper Compendium

Clickable Catalogue of Publications

November 2025

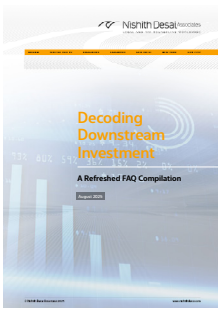
The Indian Semiconductor Ecosystem

Legal, Tax and Regulatory Pathways to Global Leadership

October 2025

Patent Blind Spots in India's Startup and MSME Landscape

Structural Barriers and Strategic Remedies



August 2025

Decoding Downstream Investment

A Refreshed FAQ Compilation

June 2025

Mergers & Acquisitions

An Indian Legal, Regulatory and Tax Perspective

For more research papers **click here**.

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

INDIA OFFICES

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

Tel +91 22 6669 5000

MUMBAI BKC

3, North Avenue, Maker Maxity
Bandra–Kurla Complex
Mumbai 400 051, India

Tel +91 22 6159 5000

BENGALURU

Prestige Loka, G01, 7/1 Brunton Rd
Bengaluru 560 025, India

Tel +91 80 6693 5000O

NEW DELHI

13-H, Hansalaya Building, 15
Barakhamba Road, Connaught Place
New Delhi 110 001, India

Tel +91 11 4906 5000

GIFT CITY

408, 4th Floor, Pragya Towers
GIFT City, Gandhinagar
Gujarat 382 355, India

FOREIGN OFFICES

NEW YORK

1185 6th Avenue, Suite 326
New York, NY 10036, USA

Tel +1 212 464 7050

SILICON VALLEY

220 S California Ave., Suite 201
Palo Alto, California 94306, USA

Tel +1 650 325 7100

SINGAPORE

Level 24, CapitaGreen
138 Market St
Singapore 048 946

Tel +65 6550 9855

BOSTON

Cambridge Innovation Center,
1 Broadway, Cambridge,
MA 02139

Cross-Border Compliance in Fintech

Navigating India's DPDPA and the U.S. Sectoral Regime towards a framework for the BFSI Sector

concierge@nishithdesai.com